DOI : https://doi.org/10.56452/223

ISSN: 0974-5823 Vol. 6 (Special Issue, Nov.-Dec. 2021)

International Journal of Mechanical Engineering

Digital Revolution and Privacy Policy

Dr. Aditi Abhyankar

Associate Professor, Economics, Ramnarain Ruia Autonomous College, Mumbai

Abstract

In Germany, around 1440, goldsmith Johannes Gutenberg invented the movable-type printing press, which brought in the Printing Revolution. And today, we are experiencing a Digital Revolution, the shift from mechanical and analogue electronic technology to digital electronics that began in the later half of the 20th century. It was made possible by the adoption and proliferation of digital computers and digital record-keeping, and it continues to upgrade itself all the time. The sweeping changes brought about by the digital computing and communication technologies which may be regarded as the Digital Revolution marked the beginning of the Information Age.

The information age, experienced at an unprecedented pace and magnitude has made comprehension of the data much difficult, and even more difficult is the challenge to protect the rights and interests of people in the cyberspace.

'Data' refers to the information that is communicated through multiple entities/persons digitally and 'Personal Data' is that piece of information without which that person cannot be identified. Data will be amongst the key drivers of economy and will create inestimable wealth in the foreseeable near future. It is therefore necessary to respect an individual's privacy related with the collection, use and dissemination of data.

This paper tries to look into the the Personal Data Protection Bill (2019), aimed at preventing surveillance capitalism from coming in way of the 'fundamental right to privacy'. The paper acknowledges how data associated with national identification - Aadhaar - has been beneficial in passing on the benefits of various schemes by engaging people with the authorities. Challenges of maintaining, protecting and verifying documents in assorted databases containing gargantuan information linked to a single Aadhaar number is discussed. The paper mentions new ideas and solutions that could ultimately converge to the ethical, building trust among citizens and the state. The paper discusses the 'right to be forgotten' that is being practised to control the untold wealth created by the Googles and Amazons of the world. The need for increase in use of blockchain technology by the government for maintaining an immutable record and securely authenticating documents in public domain also has been discussed.

KEYWORDS: Data Revolution, Privacy Policy, Personal Rights, Personal Data Protection Bill (2019), National Identification - Aadhaar, Blockchain

INTRODUCTION

The digital revolution India experiences today is brought about by the increase in the availability of data. The fluidity of using data in any field has made it the bedrock of many decisions around us. It is therefore crucial to protect the rights and interests of citizens and defend the adversities posed by this data revolution of the 21st century. This is most essential as millions of individuals are participants of this digital revolution in their everyday life and business.

This revolution has made interactions between multiple entities seamless and efficient. In case of governance, this increase in efficiency has removed barriers in providing government services. The critical reason for gain in productivity is at the junction of using data as a public good, and the key for making this digital revolution a successful one lies in the strategic use of data in policy, planning and operations. Given the level of digital infrastructure in India, it has become difficult to prevent the adverse and malicious use of technologies on the dependents of digitalisation

DOI : https://doi.org/10.56452/223

India is one of the biggest and fastest-growing digital markets in the world. The ‘Digital India’ programme, launched in July 2015, is a flagship programme of the Government of India with a vision of transforming India into a digitally empowered society and knowledge economy. With nearly 1.2 billion mobile subscriptions and 560 million internet subscriptions, India is home to the second-largest mobile subscription base in the world and the second-largest internet.

The adoption of digital technologies has resulted in a boost in economic productivity, new skills and jobs and enhanced opportunities to individuals and businesses in today’s globalised era. The Digital Revolution has come with its fair share of negative and positive factors. The positive ones being better access to information to all, easier communication and greater interconnectedness. On the negative side, it has resulted in Information overload; caused rise in Internet predators, social isolation and has challenged the personal privacy. Personal computing and other non-work related digital activities in the workplace thus helped lead to stronger forms of privacy invasion, such as keystroke recording and information filtering applications (spyware and content-control software).

Digital Revolution and Personal Privacy Concerns

Most of us use the internet every day, for work, for learnung, for shopping, to socialise, to watch films and listen to music, and to access vital services like banking and welfare benefits. The internet has the potential to support freedom of expression, the right to education, freedom of association and participation in social campaign and even political elections.

With the digital revolution, the powers of communication and information sharing have been greatly expanded and with it new technologies that can exploit the information concerned have also cropped up. The major concerns are- the risk to our right to privacy, and the risk of discrimination, which arises from how private agencies and companies collect and use our data online. The companies wish to obtain all the possible information about individuals as possible, which they can effectively use in advertising to maximise their revenue. The Government must ensure that there is robust regulation over how our data can be collected and used, and that regulation must be stringently enforced.

When using different web services and social media platforms, the vast majority of individuals would find it almost impossible to know what they are consenting to as they are highly unlikely to read and/or fully understand complex erms and conditions or privacy notices. These notices are nonnegotiable and offered in a take it-or-leave-it manner. The social media apps such as Facebook, Snapchat, YouTube and many others make joining a service conditional on agreeing the terms and conditions, which includes current privacy notices and future changes to terms. The individuals often have no choice but to agree if they want to use a service, which raises questions about whether or not consent has really been given.

Privacy International (PI) a London based leading charity advocating for strong national, regional, and international laws that protect the right to privacy around the world challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. PI investigated how peoples’ personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It mentions that privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built.

The US follows a laissez-faire approach and does not have an overarching data protection framework. US courts however, have collectively recognised a right to privacy by piecing together the limited privacy protections reflected in the First, Fourth, Fifth and Fourteenth Amendments to the US Constitution.

The EU, has recently enacted the EU GDPR, which has come into force on 25 May 2018. replacing the Data Protection Directive of 1995. It mentions, the collection, generation, use, and storage of personal data by private companies threaten peoples’ right to private and family life (Article 8 European Convention of Human Rights (“ECHR”)), as well as freedom of expression (Article 10 ECHR), freedom of association (Article 11 ECHR), and non-discrimination (Article 14 ECHR). The EU Charter of Fundamental Rights also enshrines many relevant rights, including the right to privacy and the right to the protection of personal data, in Articles 7 and 8 respectively.

The United Nations High Commissioner for Human Rights has affirmed that states are obligated to exercise regulatory jurisdiction over private companies to ensure that human rights protections extend to people whose

DOI : https://doi.org/10.56452/223

privacy is impacted by the companies generating, collecting, and using their personal data. The States are further obligated to "mitigate the impact on human rights from . . . power and information asymmetries" that exist between people and private companies in the use of peoples' personal data. It is necessary to create restraints on potential abuses arising from the vast accumulation of data, limiting how data is used to construct profiles and to make decisions about people, groups, and societies, a reedressal mechanisms for individuals, groups and civil society representing their interests.

The right to privacy is an element of various legal traditions to restrain governmental and private actions that threaten the privacy of individuals. Over 150 national constitutions mention the right to privacy.

The world is brimming with data – its magnitude and pace unprecedented. Apart from creating enormous wealth for entities having vast reservoirs of data and improved assistance in governance through increased availability of information about citizens, the ethical boundaries of data collection and processing need to be clearly defined.

With more information at disposal, patterns in identification of criminal activity through emerging technologies like facial recognition and sophisticated use of biometric data have become easier than ever before.

Blockchain, a technology which radically changes the way data is stored and managed, will be an important aspect to be considered while execution of public services in the ongoing digital revolution.

The Personal Data Protection Bill (2019)

After being worked upon for more than two years, the Personal Data Protection Bill (PDPB) was cleared by the Union Cabinet, Government of India on 4th December 2019. The PDPB is a comprehensive draft containing data protection laws which, "… provides protection of privacy of individuals relating to their personal data, specifies flow and usage of personal data, protects rights of individuals whose personal data are processed, … and to establish a Data Protection Authority of India for the said purposes…"

In the PDPB, data means the information that is communicated through multiple entities/persons digitally and personal data is that piece of information without which that person cannot be identified. Among other regulations, the amended draft stated that data can be processed or shared by any other entity only after consent, the financial and critical data (yet to be notified by Central Government) of an individual has to be stored in India, and the sensitive data has to be stored in India but can be processed outside with consent. The draft bill described financial data as the personal data with relationship to any financial institution. Sensitive data is described as the information which may constitute financial data, health data, genetic data, religious or political belief or affiliation, caste or tribe, sexual orientation, biometric data, sex life, official identifier, intersex status, transgender status, and any other data categorised sensitive under section 15.

The amended draft clearly stated that the personal data should not be collected beyond the necessary period to satisfy the purpose for collection of that information, and the personal data has to be deleted once the purpose if satisfied. Apart from other conditions stated for transfer of personal data and penalties for violations of regulations, the PDPB gives the government the power to obtain any anonymized personal data or non-personal data from companies to better deliver services to citizens. The bill provides a new definition of anonymization, thereby making sure that the process of transforming personal data is irreversible.

These being the major highlights of the Draft Bill, they make sure that the guidelines would help in providing necessary rights of people in the cyberspace and protect their privacy. The bill also encourages innovation in fields of artificial intelligence and machine learning, amongst other emerging technologies for their use in favour of public interest. Justice B. N. Srikrishna, chairman of committee which drafted the PDPB, has said, "The data protection law will be like a new shoe, tight in the beginning but comfortable eventually." However, with respect to the exact definition of critical data and sharing of anonymised data with the government, there seems to be a concern regarding violation of privacy and introduction of surveillance capitalism.

The Right to be Forgotten

The Personal Data Protection Bill (PDPB) has a section on the Right to be Forgotten and the scenarios under which it is applicable. Citizens will have the "right to restrict or prevent continuing disclosure of personal data." There are debates on this matter if the right to be forgotten for an individual prevents the right to information of

DOI : https://doi.org/10.56452/223

any other citizen. Elaboration and deliberation on this right will be important in striking the most robust data protection policy for India. Further, it is well understood that as entities start accumulating more data, it leads to increase in their control. Therefore, the PDPB's right to be forgotten has to be regulated bearing this reality.

Creation of National Facial Recognition System

The violation in privacy owing to use of facial recognition for governance or criminal surveillance purposes has been debated a lot. A facial recognition system is a technology capable of identifying or verifying a person from a digital image or a video. The reason for this is partly due to adoption of this technology in China at an unprecedented scale. The Chinese Government is using facial recognition to spot criminals in public spaces, for getting a new mobile number, for social profiling, to rate individuals based on their performance in facial recognition audits, and more.

The use of this technology is benevolent in expanding the reach of government efforts in providing services to population hitherto neglected. At the same time, it can be malevolent as it contributes to more personal information leakage and can be dangerously invasive. Currently, the National Crime Records Bureau (NCRB) of India is in the process of installing facial recognition system to track and catch criminals. The use of this technology, according to NCRB is "An effort in direction of modernising the police force, information gathering, criminal identification, verification and its dissemination among various police organisations and units across country." According to the bid document of NCRB, the facial recognition will be powered by software of private companies and images will be provided by the installed closed-circuit cameras in public spaces. The document also says that the system should be able to compensate for modification made by plastic surgery, age, scars, tattoo, beards, make-up and more, and should work with images published in newspaper, videos on internet and sketches. The system will be helpful to the police personnel to check and verify the suspect with a given database of criminals. Apart from crime prevention, this technology will be beneficial in finding missing persons, unidentified dead bodies, and unknown traced persons all over the country. It has been reported that Delhi Police identified approximately three thousand missing children within a week in the trial phase. The use of facial recognition relies heavily on data obtained in form of images, and concerns over human rights and privacy loom around.

The use of this technology is feared by many cyber security experts because of its presence being governed by weak privacy laws, thereby causing discrimination due to surveillance ambitions and keeping away democratic values. Some experts also fear that this form of surveillance mechanism will enable authorities to supress certain group of individuals. Also, any data leak to malicious persons when facial recognition is in use will provide them unlimited leverage because of access to details of 1.2 billion people in the country. Therefore, facial recognition technology should be applied judiciously, and fine line should be drawn between it being used as a public good and it being used as a surveillance technology.

National Identity

Nearly every country on this planet has some or the other form of an identity system. A national identity system associated with every citizen is vital for governance and security. In India, national identification through use of Aadhaar has been at forefront of digital revolution and empowering citizens to directly engage with the state through e-governance. E-governance has made passing on the benefits – in the form of subsidies, insurance, education and other direct benefit transfers, wages to labourers, etc – more efficient by eliminating delay in delivery or non-delivery of public services. A robust and immutable national identity is vital to ensure that citizens do not misuse the system with duplication, which can lead to terrible economic damage.

Aadhaar has served as the most important identification for citizens in the ongoing digital revolution. Aadhar, India's biometric ID database of billions of people, is linked together with other databases containing tax records, credit card transactions, travel records, vehicle information, insurance details, investment information, and more. Strict data security measures to prevent malevolent access to personal information and location of every Indian citizen, along with policy measures to disable surveillance and targeted damage by authorities are crucial to respect privacy of individuals. This fact explains the scepticism of many experts on security of Aadhaar database.

DOI : https://doi.org/10.56452/223

Few of the major projects launched by the Government of India using some of the databases mentioned above include Digi Yatra and National Intelligence Grid. According to the Ministry of Civil Aviation, during Digi Yatra – or digital processing of passengers at airports – passengers will be automatically processed based on facial recognition system at check points like Entry Point, Entry into Security check, and Aircraft Boarding. This service facilitates self-bag drop and check-in, so that travel is paperless and identity check is avoided multiple times. This is done through biometric data in Aadhaar verified against the name, mobile number, email address, and date of birth in some national database. This service is currently available in some airports, which include the ones in Delhi, Bangalore, Kolkata, Varanasi; and the service will roll out at all major airports in the years to come.

National Intelligence Grid (NATGRID) is a project by Ministry of Home Affairs (MoHA) that would link databases related to immigration, banking, individual taxpayers, air flyers, train travellers, and other general intelligence inputs. The purpose of NATGRID is to track any terror suspect and prevent terrorist attacks with real time data. The need for NATGRID came after the Mumbai attacks of 2009 and the MoHA has stressed the need for its immediate operationalisation. Apart from these, various projects have been announced to use data as a public good – some of them being the National Data and Analytics Platform by NITI Aayog, Indian Urban Data Exchange by the Smart Cities Commission, and DISHA Dashboard by the Ministry of Rural Development

Considering the number of databases and the herculean amount of information residing in those databases, it has become imperative to monitor the risks related, even if any one part of a database is compromised. Building of resilient cyber infrastructure and strict limitations on use of data beyond the specified purpose is critical to fend off major challenges relating to use of technologies relying on data and the associated technological supply chain.

Covid 19 Pandemic

All sectors, in addition to banking and finance, be it education, hospitality, media or business adopted the digital technology extensively during the Pandemic of Covid 19. As a result of the viral outbreak, an increase in digital payments is seen across online grocery stores, small retail outlets, online pharmacies, and paying bills. Contactless payments, as made with QR codes, wallets, UPI, or contactless cards, are getting recognition because they provide ease, security and allow users to maintain social distancing.

Since the beginning of the pandemic, India has provided a huhe $5 billion cash benefits to its most vulnerable citizens solely through digital payments. When the pandemic struck, the country was already on a digital-first path, with one of the largest volumes of digital transactions globally, which accelerated the adoption of contactless digital technologies. The enormous volume of digitalisation and the huge population size adopting it, further sets challenges pertaining to security, privacy and smooth functiong of the systems.

Blockchain

Blockchain is a distributed database and an information sharing platform that enables multiple authoritative domains to co-operate, co-ordinate, and collaborate in a rational decision-making process. For example, consider a set of personal data (Name, Address, City, State, ZIP Code) with the associated Aadhaar number, then using a blockchain, this set of data is fed into a cryptographically protected 'block' after it has been authenticated by various authorities. This block attaches itself at the end of a chain of already existing blocks. Here, the authentication is done by multiple authorities – called nodes - like UIDAI department, the local police, the Ministry of Home Affairs, etc. The authentication by nodes is performed by solving a complicated cryptographic problem, thereby making blockchain tamper proof. In this example, if there is malicious attempt to change a particular entry in one block, it can only be done by simultaneously changing entries in all the subsequent blocks and establishing consensus among authorities once again, which is unlikely. Also, looking at the cryptographically protected block, it is impossible to guess the original input. For instance, if input for 'City' is 'Mumbai', then the block would have the entry of type: '006aopf888sdf…' With the currently available cryptographic mechanisms, there are various entries, which eliminates the possibility of guessing the original input. Blockchain, characterised by consensus, provenance, immutability, security and trust, distinguishes itself from other technologies.

In the Indian state of Maharashtra, The Thane Municipal Corporation (TMC), along with Veridoc Global India has been working on a pilot blockchain based solution for property tax assessment. Apart from increased security, integrating blockchain technology in property tax documents will aid in faster approvals and provide a single point for verifying data through original documents. This type of solution helps in reducing administrative burden, thereby reducing processing time for citizens and verification time for various authorities.

Many states in India like Maharashtra, Telangana, Andhra Pradesh have been digitising land records. However, disputes regarding ownership of a particular piece of land can be tampered even in digital form, because possession of that land dates back to many previous generations. These Indian states have proposed a solution involving digitising land records on blockchain to solve this problem.

The Election Commission of India has been working to make sure domestic workers, students and other voters can vote from anywhere in the country. To serve this objective the Centre is planning to use blockchain technology, amongst others in linkage of Aadhaar with the Voter ID. The required legal amendments are being made and using this technology ensures immutability and validity of the link between two identities.

That being said, there has to be further regulation on use of blockchain technology to make sure it is used in a way to supplement security and trust in current offerings. According to Niti Aayog's Blockchain – The India Strategy, this technology can enable ease of collaboration for enterprises and the ease of living for citizens by bringing in transparency across government and private sector interfaces. Blockchain has the potential to revamp the currently existing processes in data management and data security to unlock new sources of efficiency and value.

Conclusion

Jonathan Rosenberg said, "Data is the sword of the 21st century, those who weld it well, the Samurai."

During Covid 19 pandemic the digital revolution and all the related benefits have vitally helped in continuation of the daily routine operations and many other activities of individuals, businesses and the governments.

The concerns mentioned above regarding the security, the malevolent intent of some bad actors, transparency, and protection of rights and interests of citizens in the cyberspace provide an opportunity to build resilient systems and robust policies to counter this form of scepticism. Some of the characteristics of policy measures that we spoke about in this paper aid in sharing personal and non-personal data by discretionary consent along with protection of individual's civil rights and liberty. The technological solutions proposed in this paper also ensures the most transparent, accountable and trustworthy form of data management in delivery of public services. In this Digital Revolution, it is important that privacy and liberty coexist in the context of data being a public good.

Digital revolution has given considerable benefits to society at large, but it has also brought its fair share of concerns in the process. Powers of communication and information sharing have been greatly expanded and with it new technologies that can exploit the information concerned have also cropped up. It has ushered in a new scenario where mass surveillance can become the norm, bringing in its wake new concerns about civil and human rights.

References

1. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
2. https://corporate.cyrilamarchandblogs.com/2019/12/personal-data-protection-bill-2019-analysis-india/
3. https://www.livemint.com/Money/yO3nlG7Xj4vo2VJsmo8blL/What-is-the-right-to-be-forgotten-in-India.html
4. https://economictimes.indiatimes.com/tech/internet/worlds-biggest-face-recognition-system-arrives-in-india-next-month/articleshow/71692022.cms
5. https://www.buzzfeednews.com/article/pranavdixit/india-is-creating-a-national-facial-recognition-system-and
6. https://www.indiatoday.in/india/story/charred-body-of-police-inspector-found-in-rajasthan-s-jalore-cops-rule-out-foul-play-1649365-2020-02-24

DOI : https://doi.org/10.56452/223

7. https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf
8. https://www.globalgovernmentforum.com/india-to-develop-blockchain-voting-system/
9. United Nations Human Rights Council, The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights, 3 August 2018, A/HRC/39/29, available from https://undocs.org/A/HRC/39/29