VOLUME 4 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

# UNDERSTANDING“DATA” WITH RESPECT TO PROVISIONS FOR THE SAME IN INDIA

- Hitesh Malik[1]

## Introduction

In the past few years, there have been global stories about the Snowden disclosures and the NSA reports on government mass surveillance, the Apple-FBI controversy, and the WhatsApp-Facebook data exchange agreements. Information and Communication Technology (ICT) has revolutionized how we deal with information, do business, communicate, and interact with each other or with computers. Yen, in 2002, defined cyberspace as “the virtual space created by operation of the Internet, a network of computers that share information.” In this virtual cyberspace, interconnected computers, computer networks, and devices exchange, store and process massive amounts of personally identifiable information (PII) about individuals. PII includes social security number, name, Birth Details, parents' names, biometric records or any other information connected to a person, such as medical, economic, educational, and employment information (NIST, 2010). Various organisations in cyberspace routinely store sensitive PII of their clients. In several cases, these organisations have either been careless in handling this information or have collected and used it as a commercial commodity.

## Data Related to Privacy

*'Data' is a term of utmost importance in the context of data privacy and legal regulations. It involves the representation of knowledge, facts, ideas, opinions or directions in a manner that is appropriate for communication, understanding or processing by human beings or by automatic means;*

[1] Student at Amity Law School, Noida

Data can be further categorised into two parts, which are "Personal Data" and "sensitive personal data"

"Personal data" is defined in the GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"[2]

[3] *"Sensitive Personal Data" means personal data revealing, related to, or constituting, as may be applicable—*

*(i) Racial or ethnic origin*

*(ii) Political opinions*

*(iii) Religious or philosophical beliefs or other beliefs of a similar nature*

*(iv) Data on the Individual's Genetics*

*(v) Unique Biometric Data (For identification of an individual)*

*(vi) Financial Data*

*(vii) Passwords*

*(viii) Sexual Orientation*

*(ix) Membership of a trade union*

*(x) The commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings*

*(xi) Physical or Mental Health*

Consideration must be extended to other groups, including financial information, social security numbers and children's data. Many countries already addressed adding new data types requiring

[2] Section 3(35)

[3] GDPR, Article 4(1)

extra safety due to their 'sensitivity' to their national reference. In India, the treatment of 'caste information' as SPD. Seeing the state consider the local context and the reality is a significant step in ensuring the legislation lays down specific protection.

It is also critical that a higher degree of security applies to data that exposes SPD by profiling and the use of proxy information (for example, through using someone's buying history to imply a health condition) because such processing data suggest, extract and forecast SPD without, in addition, being expressly given to a specific persona.

## What is Data Protection?

Data protection can be described as a set of policies and laws that seek to limit the impact of the processing of data collected, stored and distributed on the privacy of such individuals. Data can be linked to wealth, fitness, character, personality, etc., allowing the compiler or consumer to recognise the data, making it easier to identify the individual.

Data protection should ensure the following:[4]

- Limitations on the collected PD must be acquired transparently and legally.

- The objectives for which the data needs to be utilised must be defined (as soon as possible) at the compilation instance and is only utilised for the reasons decided. PD can not be published, used or stored for the initial intent, either with the client's permission or by the law; it must then be removed if it is no longer needed.

- PD, as produced and stored, should be sufficient, valid and restricted to the need for the objectives for which it is to be utilised.

- The information should be absolute and finalised, and steps are to be undertaken to confirm that it is updated.

- Rational security safety measures are to protect PD from theft, unauthorised access, damage, use, alteration or release.

- There must be no hidden data, origin or computing machines. Entities should be informed of the gathering and analysis of their information, the intent for which it is used, and who controls it

[4] The Keys to Data Protection, A Guide for Policy Engagement on Data Protection by Privacy International

and who processes it.

• Individuals have a variety of responsibilities that allow the latter to regulate one’s PD and any handling that may occur.

## Need for Data Protection

The 21st century is part of the 4th generation of advances in technology and innovations, andit has seen a significant rise in the number of forms in which knowledge may be used, which is why we term this time 'the digital age.' Considering the prevailing pattern, it is estimated that humans' worldwide volume of digital data would hit approximately 44 zettabytes[5]. An enormous amount of this data will comprise private and personally identifiable information involving individuals.

With the advent and accelerated introduction of new technologies, machines are being developed and updated slowly to ingest and process vast amounts of data to determine and uncover patterns in many areas of human activity. The value of data is recognised globally by states, companies and individuals. For instance, evaluation of very vastly complex data sets is generally carried out via Big Data Analytics, which, in effect, enables organisations and corporations to invite insights into numerous relevant fields of human evolution, such as safety, food, defence, transport networks, energy conservation and urban development[6].

The 'New India' program offered by the prevailing current government has become a turning point for India, with its industrial innovation extending to a variety of fields such asgovernment,healthcare,educationalfacilities,cashlessfinancialsystemandelectronic payments, equal and fast delivery of welfare schemes, etc. to motivate its population.[7] India has roughly 450 million users, accounting for approximately 6.5 per cent of the world's population and a 7-8 per cent growth rate.

Dataiscrucialandvaluableeven thoughitisintangible,andevenwhenitisshared,itleads to increased

[5] ‘The Digital Universe of Opportunities: Rich Data and the Increasing Values of the Internet of Things’, EMC Digital Universe with Research and Analysis by IDC (April 2014)

[6] European Commission, ‘European Data Protection Reform and Big Data: Factsheet’, (2016)

[7] PIB,‘DigitalIndia– AprogramtotransformIndiaintodigitalempoweredsocietyandknowledgeeconomy’(20August2014)

effectiveness in both the public and private sectors. The reality behind the world today seems to be that India is moving into a digital environment in which almost every individual activity has a kind of data transmission process or another, which the SC acknowledges in the *Puttaswamy case*.[8]

Categorically, the development of the concept of data protection has evolved as the trinity of guardians to private data that are accessible employing various methods of extraction, disclosure and usage. This leads to issues such as data protection and valorisation of data, which begs the question of whether individuals or organisations are entitled to use private data.

A critical way forward here is to comprehend the unambiguous definition of privacy, for it may vary in the context. Three main categories of privacy have been recognised: personal area protection, territorial nothingness, and space privacy, which PD also influences. The interconnectedness of data protection and PD is implicit due to its ubiquity, although privacy and freedom of decision-making remain.

In a society that more than ever differentiates itself regarding its acceptance of single features, some aspects of the user turn out to be the most recognisable face of self-identity, like education, age, body parts or sexual orientation, if not the personalisation tendency itself. Confidentiality is admired in places where it genuinely makes spaces of life credible rather than defeating the purpose. There is an issue of releasing identifying information that provokes anger and is secret. Suppose the information is designed to correct the stereotyping and bias against individuals. In that case, the outcome is negative, does not serve the purpose, and there is the additional problem of being stereotyped and prejudiced. However, in some cases, recent research revealed that such a reason as "ethnicity", "inbuilt identity", or "absence of higher education" is still getting significant attention as a cause for immigration partition.

It might be one of the strategies of leaders to divide the large public by factors like religion, caste, etc. and make them hate each other. The state is involved with other matters that could threaten the privacy of individuals. Likewise, the government and business organisations might be so efficient in ensuring things sit quietly among the people that it can worsen for everyone by destroying the ability to think independently.

[8] JusticeK.S.Puttaswamy(Retd.)v.UnionofIndia&Ors.2017

Under Article 21 of the Constitution, the right to privacy was recently included as a fundamental right of the citizens by the Hon'ble Supreme Court of India.[9]

In addition to making this right relevant, the government must also set up a data-protection system that further protects the citizens from the hazards of privacy and confidentiality emerging from governmental and non-governmental actors and supports the greater good. It is the acknowledgement of the obligation of the government that the council must function with the formation of a framework for data protection.

The possibilities for discrimination, exemption and threat in the digital economy are equally plausible. Facebook's notable acceptance that the information collected from 87 million Facebook users, which include 5 Lakh Indian users, had been shared with Cambridge AnalyticaviaanapplicationwhichretrievedPDfromFacebookuserswhodownloadedthe application as well as from their friends demonstrates several such damages – users did not have effective control over the data. Furthermore, they had little idea that their actions would be exchanged with third parties for specific targeting of the US election ads. Sadly, the tragedy is hardly unitary or extraordinary. Data collection practices are usually opaque, entrenched in intricate, incomprehensible forms of privacy, resulting in procedures that consumers have had little influence over. Insufficient knowledge of data and subsequent spam or, worse, more tangible damage is unfortunate.

**The main features of data protection legislation should be enacted:**

- To secure the individuality of individuals about their PD.
- To clearly state where the transfer and use of PD is necessary.
- To build trust between individuals and organisations processing their personal information.
- To explicitly state the rights of individuals whose PD are processed
- Build a framework for the application of operational and technological steps for the collection of PD.
- To set down guidelines for transnational transmission of PD.

[9] Ibid

- To make the entity that processes data accountable for the collected data.
- Provide remedial measures for unlawful and detrimental processing.
- To develop a data protection department for the monitoring of data collection

## Interwoven Concept of Privacy and Data Protection

In the 1970s, electronic information systems usually contained personally identifiable information. To tackle this concern, the USA formed an Advisory Committee to discuss the numerous technical and legal assertions about the automated world information gathering. The HEW Committee issued a seminal report that advised that the Congress of the USA should adopt a Code of Fair Information Practices based on FIPPS standards. FIPPS is a collection of guidelines recommending how information must be processed, collected and administered to sustain fair treatment, security and privacy in a fast-growing international technological vanguard. FIPPS is now considered to be the foundation of advanced data protection legislation around the world.

The FIPPS soon followed the OECD Guidelines in the 1980s—the OECD Guidelines were highly influenced by FIPPS and were designed to provide a basis for harmonising federal legislation on privacy within OECD members while enshrining human rights and avoiding disruptions in global information flows. The OECD Guidelines have influenced several data protection frameworks, including the European Directive 95/46 / EC on the processing of personal information and, indeed, the free movement of such data(APEC Framework) 2004 and data security laws such as the Australian Privacy Act, 1988 and the New Zealand Privacy Act.

It was also suggested that traditional Privacy Principles weren't well equipped to meet the complexities of the exponential growth of numbers via the application of personal knowledge, advances in computers, and global data flows. This resulted in various problems, for which an expert committee was set up to revise and modernise the OE—CD Guideline. The principles of the OECD, as amended in 2013, were the consequence of this move.

The 2013 OECD Guidelines have been questioned as inherently inconsistent with emerging technology and Big Data analytics, which have transformed and changed how data is collected and stored. Currently, companies provide information that has been produced or obtained from many sources. This information collected also includes:

Financial information, workplace data and user data. However, the scenario has altered, with data being gathered and utilised unexpectedly when these ideas were developed. As a direct consequence, we were exposed to the age of digital technology and Big Data analytics.

Although big data may lack a specific description, it can often be interpreted as requiring the compilation of vast amounts of information and applying innovative techniques (like predictive analysis) to obtain data. Such data is commonly divided under 3 Vs, namely 'volume', large datasets, 'velocity' relating to real-time data, and 'variety' covering various data sources. Other technological advances, such as artificial intelligence, machine learning, and IOT, constitute the big data world. Big Data requires gathering vast amounts of data; the source of such information may not be evident to the user, and the consent may not be as substantial. Alongwith this, Data may be generated as a result of a sale or obtained by a provider in return for a free service ( e.g. unpaid e-mail accounts, social networking sites, etc.) or as a result of unpaid service ( e.g. GPS navigation) but that may not be feasible to ascertain the reason for which personal data is handled at the time of development.

The basic concept of PD has since been widened with the invention of this technology. For example, by evaluating metadata, such as a compilation of statistical or aggregated observations, or integrating previously separate data sets, Big Data has dramatically extended the spectrum of publicly recognisable data. Data regarded as non-personal information may now emerged with other data sources to produce publicly identifiable data. For example, technologies such as the IoT depend on continually gathering PD from owners of 'smart devices,' which can then be viewed as delivering specialised services. In these cases, however, it may be impossible to abide by the conventional privacy standards of permission, selection and prohibition of use. Given the growth of new technology, solutions to the traditional privacy standards currently regulating them also require careful study.