SJIF Impact Factor: 7.001| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 9 | September 2020 - Peer Reviewed Journal

EXPANDING DIMENSIONS OF DATA PROTECTION

Dr. Nandan Sharma[1]
[1] *Associate Professor, Head, School of Law, Shoolini University, Solan, Himachal Pradesh*

INTRODUCTION

The technology developed by United States (U.S.) military, during the cold war, to assist communications in the event of a nuclear attack in 1969 marked the start of the Internet. The two decades of 1980's and 1990's laid the foundation for the internet revolution. The lifting of restrictions on commercial use of the Net by National Science Foundation in U.S. allowed the use of internet for purposes other than research and education. The Internet does not simply take individuals out of their sphere, it redefines their sphere totally (Jacques Vallee,2003). Technology gives choices made by government, businessmen, and individuals. Although some special technology may be used to protect personal information and autonomy, the over-whelming tendency of advanced technology is to do the reverse. In this scenario, two forms of digital worlds are possible in the future or perhaps are already in existence - Solid State Society and the Grapevine Alternative with radically different purposes. The pervasiveness of the Internet technologies has resulted in the modern information revolution (Jonathan Zittrain, 2008). In the internet age, individuals have become "data subjects" and they fear about the protection of their sensitive information by other data subjects, government bodies or private corporates. Since the information age inevitably leads us to the rise of the individual, they may be best viewed by way of "Digital Society Personas", each of whom relates to technology and participates in society in a different way. (*Howard Rheingold*, 1993).

The dominant problem is that the organizations dealing with the identifiable personal data are the same organizations who share it online. Individuals are under two compulsions - compulsion of surveillance from government and virtual compulsion in the form of necessity to resort electronic transactions in day-today activities. The enormous information acquisition, transfer and processing power of cyberspace are viewed as exposing them all to more and more frequent and pernicious invasions of their privacy (David Baumer and J.C.Poindexter,2002). The sheer quantity of information; the ability to collect unobtrusively, aggregate, and analyze it; the ability to store it cheaply; and the ubiquity of interconnectedness are capable of eroding the protection to personal information. Transaction data – both traffic and location data deserve our particular attention (Serge Gutwirth,2009). Infringements of the recognised rights have created new concerns in human social systems cybercrime, and privacy concerns etc. They affected people's lives either directly or indirectly. Recent laws and decisions are creating millions of splintered rights in cyberspace, and these rights are destroying the commons-like character of the Internet, which has previously lead to such extraordinary innovation (Dan Hunter, 2003). The usefulness of existing rules governing cyberspace is challenged from complex cultural and national differences across the globe.

Legal solutions must acclimatize against the realities of the Internet and cyberspace. In modern cyberspace, an absence of rules (or at least enforcement) has led both to a generative blossoming and to a new round of challenges at multiple layers (Jonathan Zittrain, 2008). The sorry state of computer privacy and security can be checked by culmination of efforts from technologists, business acumen, administrators, legal professionals and much more.

MULTIFARIOUS ASPECTS OF PERSONAL DATA WITH SPECIAL REFERENCE TO CHARACTERISTICS, APPROACHES AND USE

In information societies, identity-relevant information look like guns and ammunition leading to theft, identity fraud or straightforward harm using the information (Jeroen van den Hoven,2008). At the same time, information can also be used for the advantage of the society. Data may be collected before, during, or after a business transaction and data collection may be known or unknown by the consumer. A productive use of information is one that makes it more valuable, including collaboration,

SJIF Impact Factor: 7.001| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 9 | September 2020 - Peer Reviewed Journal

remixing, and validation. Destructive uses leave the information less valuable, and include misrepresentation, misidentification and dilution.

1. Concept, Definition and Classification of Personal Data

Data are constructs from facts, from social processes of definition, selection, and collection. They serve and are defined by, interests, and relate to the purpose of their construction. They are only capable of being comprehended in the social context What constitutes as data will differ from context to context. Data always have a purpose - they serve interests and those purposes are crucial in their definition, selection and collection and in deciding what is done with and to them. The key point is that data cannot be understood outside of the social contexts of their construction and the interests that they are proposed to serve.

(a) Meaning and Definition of Personal Data

"Personal information consists of those facts, communications or opinions which relate to the individual and which he may consider as *intimate or sensitive* and therefore to want to reserve or at least *restrict* their collection ,use or circulation" (Raymond Wacks, 2010). Facts are not confined to textual data, but encompass a wide range of information, including images, DNA and genetic and biometric data such as fingertips, face and iris recognition, and the ever-increasing types of information about us. On its own, an item of information may be perfectly *innocuous,* but when combined with another piece of equally inoffensive data, the information is transformed into something genuinely private. In any event, no item of information is in and of itself personal. An anonymous medical file, bank statement or lurid disclosure of a sexual affair is harmless until linked to an individual and only when the identity of the subject of the information is exposed, it become personal. The norms determining the nature of information are culture-relative as well as variable. Privateness is not an attribute of the information itself, the same information may be regarded as very private in one context and not so private or private at all in another.

(b) Classification of Personal Data

Table-2.2: Sensitive Data under Primary International Instruments

Sr.No.	Council of Europe Convention 1981,	UN Guidelines,1990	EU Data Protection Directive,1995
1.	Racial origin	Racial or Ethnic origin	Racial or ethnic origin
2.	Political opinions	Political opinions	Political opinions
3.	Religious or other beliefs	Religious/philosophical/other beliefs	Religious and philosophical beliefs
4.	Sexual life data /Sex life	Sex life	Sex life
5.	Health data	-	Health
6	-	Membership of an association and Membership of a trade union	Trade-union membership
7.	-	Colour	-
8.	Criminal convictions	-	-

Table 2.2 points out the sensitive data as defined expressly under Council of Europe Convention, 1981, UN Guidelines,1990 and EU Data Protection Directive,1995. It further shows that racial origin, political opinions, religious/philosophical beliefs and sex life are the four common data in all three instruments. Whereas criminal convictions found place only under Council of Europe Convention 1981; colour only under UN Guidelines,1990 ; and health as well as membership of trade union under two of them.

(i) Sensitive Data as a Special Category of Protected Data

Certain items of personal information are intrinsically more sensitive than others and therefore warrant stronger protection. The term sensitive data was originally used under the Council of Europe Convention 1981 on Personal Data. Sensitive data means personal data denoting racial origin, political opinions or religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life. Thus, personal data has been categorised as sensitive data due to its very sensitive character. Swiss Federal Data Protection Act, 1992 protects Personality profiles under Article 12. Personality profiles are collections of data that allow the appraisal of essential characteristics of the personality of an individual (for example, personnel files often fall into this category). The various words used - "revealing", "referring to", "relating to", "as to", "on" appear to be very similar, however, the terms can have implications, in particular as concerns

SJIF Impact Factor: 7.001| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 9 | September 2020 - Peer Reviewed Journal

matters which can be said to indirectly "reveal" certain sensitive matters.

The logic of sensitivity seems to imply that all data concerned should be subject to the same degree of restriction. Sensitivity lists must be phrased in a way that unmistakably indicates their purely exemplary character and their components can hence always be complemented or replaced. Contextualized Approach to Sensitive Data contends that personal data becomes sensitive according to its context, which was formerly adopted by countries such as Austria and Germany. It is an abstract categorization. Purpose Based Approach to Sensitive Data considers the purpose underlying the processing of personal data, that is, whether the processing is intended to reveal sensitive data. It has been advocated by the various regional and national organizations. All data must consequently be assessed against the background of the context that determines their use. The specific interests of the controller as well as of the potential recipients of the data, the aims for which the data are collected, the conditions of the processing and its possible consequences for the persons are factors that, put together, allow both the range and effects of the processing to be discerned and thus to determine its degree of sensitivity. At present, only purpose based approach holds prominence and is widely accepted.

(ii) Personal Identifiable Information (Data)

Personal Identifiable Information (Data) is a central concept in data protection law and requires a broad definition in light of modern technologies involving data mining and behavioral marketing (Paul M. Schwartz and Daniel J. Solove, 2011). Technology is now posing a considerable challenge to the non-PII side of the dichotomy and the wide availability of so much information about people heightens the ability to turn non-personally identifiable information into one. The broadness must be clear so as to avoid encompassing nearly all information. **Table 2.3** below provides the reflection of three kinds of approaches to Personal Identifiable Information in brief.

Table – 2.3 : Approaches to Personal Identifiable Information

Sr.No.	Approach	Standard
1.	Tautological Approach	Any information that identifies a person
2.	Non-public Approach	Focus on what PII is not rather than on what it is
3.	Specific-types Approach	If the information falls into an enumerated group, it becomes a kind of statutory "per se" PII

The model places information on a continuum that begins with no risk of identification at one end, and ends with identified individuals at the other. Under the PII 2.0 model, information can be about an identified, identifiable or non-identifiable person. A person has been recognized when her identity is ascertained; an individual is identifiable when there is some non-remote possibility of future identification. The risk level for such information is low to moderate and non-identifiable information carries only a remote risk of identification. When information refers to an identified person, all of the Fair Information Practices generally should apply. The key Fair Information Practices data security, transparency and data quality.

Table – 2.4: Personal Information and Relationship with Individual (Jerry Kang,1998)

Sr.No.	Relationship of Information with Individual	Information	Examples
1.	Authorship Relationship	Individual could have purposefully created or prepared the information typically to communicate that information to another party	A SMS created for some close person
2.	Descriptive Relation	Information could describe the individual in some manner such as could speak to some permanent or non-fleeting status of the individual, either biological or social	Age of individual, Medical condition etc.
3.	Instrumental Mapping Relation	Information primarily linked to the individual for institutional identification, secured access, or provision of some service or good	Login username or password of Bank account

SJIF Impact Factor: 7.001| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 9 | September 2020 - Peer Reviewed Journal

Information can be identifiable to an individual in three ways: it can bear an authorship relation to the individual, a descriptive relation to the individual, or an instrumental mapping relation to the individual. The detailed information in this regard is reproduced in **Table 2.4** with examples.

CONCEPTUALIZATION, GENESIS AND PRINCIPLES OF DATA PROTECTION

Technological advancements not only lead to benefits, but new threats for our open society. The privacy laws that many governments have reasonably instituted to protect their citizens from having their personal information flow outside the control of the laws of their nation raises many difficulties when engaged in an Internet environment. Information privacy" or "data protection" were considered as discrete legal or technological issues. Data means representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer. With the growth of digital age, more and more personal information of consumers, citizens finds its way into massive databases held by the private sector, and the governments. The modern society depends for its survival on the use of personal information and this use is increasingly assuming a multi-national dimension adds fuel to the problem.

(a) Genesis of the Concept of Data Protection

The introduction of data banks in computers posed a threat to individual privacy and required methods to control the misuse of the technology. Personal privacy, as it relates to personal-data record keeping must be understood in terms of a concept of mutuality. The nomenclature "data protection" is derived from the German term "Datenschutz". The realization that this nomenclature is problematic in several respects has resulted in increasing supplement by the term "data privacy". The first law was enacted in the Land of Hesse in Germany in 1970. Sweden was the second country to introduce data protection legislation, with the Data Act, 1973. This Act regulated the automated processing of files containing personal data.

The development of data-protection norms is generational falling in four periods from 1970s till present. The shift from economic to broad-based political union brought with it new and more urgent attention to the protection of informational privacy. The first-generation data-protection norms adopted functional look at data processing society, where data protection is seen as a tool specifically designed to counter the dangers that emerge from the use of computers. The statutes used the term "data" in "data banks". Data protection statutes in the second generation witnessed re-orientation of data protection from technology regulation to individual liberty and freedom. Words such as "privacy" and "information protection" were employed instead of technical jargons: "data," "data bank," "data record," "data base," "data file." The third generation of data protection emphasized informational participation and self-determination. The fourth generation witnessed amendments taking into account philosophical and ideological transformations. In the 1970s and the 1980s, when omnibus data-protection policy was confined to Western European societies, it was possible for some commentators in Canada, Australia, and the United States to argue plausibly that this legislation was a feature of a continental (civil) legal system, and that the Anglo-American system dictated a less regulatory regime that placed more responsibility on the individual citizen to demonstrate damage and make a claim through the courts. The online privacy has gained momentum only after 1990s.

Principles of Data Protection

At the core of data-protection legislation is the proposition that data relating to identifiable individual should not be collected in the absence of the genuine purpose and the consent of the individual concerned. Data Protection Statutes routinely stipulate that personal data must be collected by means that are both lawful and fair. Personal data may be used or disclosed only for the purposes for which the data were collected for or some directly related purposes, unless the data subjects consents.

Data protection laws have much the same aim and function that *policies of 'sustainable development*' have in the field of environmental protection. They seek to safeguard the privacy and related interests of data subjects at the same time as they seek to secure the legitimate interests of data controllers in processing personal data just as policies of 'sustainable development' seek to preserve the natural environment at the same time as they allow for economic growth. Data protection instruments are expressly concerned with setting standards for the quality of personal information which breaks down into a multiplicity of interests. They tend to seek to manage most established systems of administration, organisation and control of information allowing processing of information about others for various legitimate ends. In its early stages, data protection laws tended to apply almost exclusively to textual information, now the developments in technology

SJIF Impact Factor: 7.001| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 9 | September 2020 - Peer Reviewed Journal

have allowed any form of recorded information to come within the ambit of the legislation. Video images recorded by means of CCTV or similar camera systems ; and the biometric data collected are also granted shelter by the data protection statutes.

ELECTRONIC TRANSACTIONS

Information is collected by employees, voluntarily given by individuals at social media platforms and is of strategic nature available with the Government. Such information is often stored in electronic form and is also subject to loss.

(a) Transactions at the Hands of Employees

Employers collect personal data on job applicants and workers for a number of purposes: to comply with law; to assist in selection for employment, training and promotion; to ensure personal safety, personal security, quality control, customer service and the protection of property. There is a need to develop data protection provisions which specifically address the use of workers' personal data.

(b) Transactions at the Hands of Nation-States: Security Versus Autonomy

Telecommunications, energy, banking and finance, transportation, water, emergency services, and essential government service are in e form in this "wired" age. The absence of international conventions, addressing cyber warfare – Third Wave warfare raises concerns for States (Isaac Ben-Israel and Lior Tabansky, 2011). The computer warfare gives the attacker an advantage over the defender, unlike the conventional warfare.

(c) Social Media Platforms

The two-way interactive experience has been made possible by social media. The data subjects are themselves the originators or the authors of the proffered information. Certain privacy-related terms and conditions may apply depending on the specific social media activities or functionality a company leverages *within a social media platform*. The culture of sharing present on social media sites itself can lead to over-disclosure by employees, and the pure volume of data that can be mined from social media sites may allow competitors and criminals to connect-the-dots to reveal confidential or sensitive information.

The ease with which users reveal personal information in social networking services, as well as the simultaneous lack of awareness and understanding regarding the threats and dangers lurking in such disclosure of personal information, alarmed It is thus essential to rebalance the rights and obligations of both the providers of services and the users, to empower the user via technological tools and to create privacy-friendly default settings.

Sum-Up

The study has summarized the impact of the information revolution on the dimensions of information subject to protection at domestic and international levels. It discussed that the expression personal data must be given a wider interpretation in the light of new technologies. Attributively used descriptions may in coming times fall under the ambit of personal data. Both risks and benefits are associated with the collection and used of personal data without the consent of the data subject. There is a current and accelerating "personal information alienation," and that alienated information is being put to use in increasingly expansive ways that affect the individual to whom they pertain. The data subjects and data processors need to be placed on equal footing in determining how and when personal data may be converted into commercially viable products in the information marketplace.

Paul M. Schwartz and Daniel J. Solove have proposed that the necessary legal protections should generally be different for identified and identifiable data against the prevalent reductionist and expansionist approaches. In the reductionist view (adopted by United States , the tendency is to consider PII as only that personal data that has been specifically associated with a specific person, leaving too much personal information without legal protections. The expansionist approach treats identified and identifiable data as equivalent.

REFERENCES

1. *Jacques Vallee, The Heart of the Internet: An Insider's View of the Origin and Promise of the On-Line Revolution, 3(Hampton Roads Publishing Co, Inc, Charlottesville, 2003).*
2. *Jonathan Zittrain, The Future of the Internet-And How to Stop It, 8 (Yale University Press, London, 2008).*
3. *Howard Rheingold, "Virtual Communities- A Slice of Life in My Virtual Community" 58, Linda Marie Harasim (ed.) Global Networks: Computers and Internatinal Communication (MIT Press, 1993).*
4. *David Baumer and J.C.Poindexter, Cyberlaw and E-Commerce 161, (McGraw-Hill, Syndeny, 2002).*
5. *Serge Gutwirth, Reinventing Data Protection? vi Serge Gutwirth, Yves Poullet, Paul de Hert, Cécile de Terwangne, Sjaak Nouwt (eds.) (Springer,2009).*
6. *Dan Hunter , "Cyberspace as Place, and the Tragedy of The Digital Anticommons" , 91 (2) California Law Review, 439 (2003) at 444.*
7. *Jeroen van den Hoven, "Information Technology, Privacy and The Protection of personal Data" 311 Jeroen Vanden Hoven & Weckert (eds.), Information Technology and Moral Philosophy (Cambridge University Press, 2008).*

SJIF Impact Factor: 7.001| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 9 | September 2020 - Peer Reviewed Journal

8. *Raymond Wacks, Privacy- A Very Short Introduction, 47(Oxford University, New York, 2010).*
9. *James Waldo, Herbert S. Lin & Lynette I. Millett (eds.) Engaging Privacy and Information Technology in a Digital Age 39-40 (National Academic Press, Wahington,2007)..*
10. *Paul M. Schwartz and Daniel J. Solove , "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", 86 New York University Law Review 1814 (2011) at 1827. One to one marketing is overtaking the traditional mass marketing , requiring recording a person's behavior, analyzing it, and making the kinds of offers based on the patterns that emerge from this collected data.*
11. *Jerry Kang "Information Privacy in Cyberspace Transactions", 50 Stanford Law Review 1193 (1998) at 1208.*
12. *Isaac Ben-Israel and Lior Tabansky , "An Interdisciplinary Look at Security Challenges in the Information Age" 3(3)Military and Strategic Affairs 21 (2011) at 33.*