VOLUME 2 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

TRANS BORDER DATA FLOWS IN TECHNOLOGY TRANSFER

- Aranya Nath, Sweta Pal & Antara Paral[1]

ABSTRACT

Transborder Data can be carried out through streamlined motion statistics in the form of Electronic mail, online Transfer, immediate changes in the business, and innovative conditions for data flow preparing is additionally occurring, driven through advancements, for example, the multiplied globalization of the world economy; the creating economic magnitude of facts flows managing the universality of data flows moves over the Internet; more prominent direct inclusion of people in transborder data flows streams; the altering job of topography; and growing risks to the safety of people. Regardless of these central adjustments in the records flows getting ready scene. The improvement in the tenet of Trans border facts flows streams in a variety of nations, there has been little undertaking, so a long way to lead a deliberate inventory of such guidelines at a worldwide level; to appear at the techniques hidden it, and to assume about whether or not these tactics need to be rethought. This investigation is supposed to portray the current status of Transborder facts flows circulation guideline and to incite reflection about its points, activity, and adequacy, at present and later on.

Keywords: Trans-border Data Flows, Technology Transfer, Online Economy, Internet, E-commerce.

INTRODUCTION

Earlier, the data was transferred through point-to-point transfer. There was no internet around 30 years ago.[2] But now a day, with the impact of globalization, transactions are initiated through the internet and mobile banking that encompass NEFT, Online transfer, Google Pay, and so forth. A couple of data flows co-occur via social networking, search engine, and cloud computing.[3] This has led to facts transfers over the internet, and extended monetary significance of the information process, with the direct involvement of human beings in Trans border

[1] Student at GITAM University, KIIT University & IFIM Law School Respectively.
[2] Christopher Kuner, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 3-22 (2013)
[3] Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning? 3 International Data Privacy Law Journal, Oxford University Press,74, 2012

information, flows. Whereas this can be exposing human beings to a lot of privacy risks, it is conjointly tricky for businesses that are series the data at once entered via users or via their movements while not their information - e.g., internet surfboarding, e-banking, or e-commerce – and correlating regular via a lot of superior analytic equipment to get an amount out of data. The latter are in manage of expertise assortment and its use, on account that information has grown to be one of the drivers of the understanding mainly based totally on society that is altering into even a lot of imperative to enterprise than capital and labor.

On the contrary hand, the private area uses non-public expertise to structure new needs and construct relationships for producing income from their services. Human beings are put out their knowledge on the online reciprocally for beneficial offerings at almost no price. However, at some stage in this modified paradigm, the private sector and civil society want to construct prison regimes and practices that are clear and encourage confidence amongst people and decorate their potential to adjust get right of entry to their knowledge. At the same time, quantity is generated from such knowledge assortment and technique for all players.

Today's world is a world of technological development at any place

every second day, we tend to see new technologies coming back to the fore and sitting myriad unknown challenges. This can be an age anywhere technology is taking a giant leap vis-à- vis law concerning it, a period where the intangible property is extraordinarily lucrative. Info has become a primary plus, a crucial aspect for the improvement of records economy and additionally, the non-public statistics are the proper use of this plus. The non-public data command by the data method incorporation will become a precious fabric whose misuse or abuse invades the desirable privacy of people or a company. The upward push inside the worth of such data entails demand of a good and effective prison regime for protecting such private knowledge, henceforward reconciliation the requirements of the individual, commerce, and society as an entire.

EVOLUTIONOFCURRENTDATASECURITYREGIMEININDIA

In India, there still is no no privacy law regulation. In India, there are numerous legislation which involve data encryption both intrinsically and extrinsically. India is mainly controlled by the "*Indian Constitution, the Information Technology Act of 2000, the Credit Information Firms (Regulations) Act of 2005 (CICRA 2005), and the Information Technology Information Technology Rules 2011.*" Out of those numerous statutes the one that directly deals with data protection is[i]. Once the "Information Technology Act 2000" was passed, the concept-ofinformationprotectionwasn'tenvisaged. Under *"Indian constitution Right to privacy enshrined*

in Article 21": Right to privacy enshrined in Article 21: The concept of confidentiality acknowledges the inalienable freedom to be alone and to have unfettered access to his own area. The concept 'confidentiality' refers to an individuals personal right to determine how much of himself he wants to disclose with others, as well as his control over the time, place, and circumstances under which he speaks with others. It means he has the right to withdraw or participate as he sees appropriate. It also refers to the individual's right to control the broadcast of information about him because it is his personal property. The person is the primary concern when it comes to privacy. As a result, it is related to and overlaps with the concept of liberty. Utmost confidentiality proponents might acknowledge that there are approaches to achieving with establishing the basis and breadth of the correct. Confidentiality and liberty must be viewed in the context of many other rights and principles.[4] The right to privacy emerged as an active and unique principle in the domain of actusreus law, whereby a novel ground of claim for negligence deriving from illegal intrusion of dignity was established. The privilege includes two parameters that become, essentially, two sides to this argument:

1. The general law of privacy, which provides a res judicata action for damages resulting from an unlawful invasion of private, and
2. The fundamental concept of privacy, which offers a res judicata suit for damages resulting from an illegal intrusion of private.

The very first aspect of this right should be claimed to already be broken whenever, for illustration, a person's name or face is used without his knowledge for promoting or quasi responsibilities, or his narrative is written, whether praising or otherwise, and exposed without his consent. However, in past few decades, this ability has already been granted quasi constitutional recognition.[5] India is a contributor to the "*International Covenant on Civil and Political Rights, which was established in 1966. Article 17 of the Convention guarantees the 'right to privacy.' Article 12 of the 1948 Universal Declaration of Human Rights is virtually identical. Article 17 of the International Covenant is not in conflict with any provision of our municipal legislation. As a result, Article 21 of the Constitution*" must be construed in accordance with international law.[6]

DATA PROTECTION & PRIVACY ISSUES IN CYBERSPACE

DIGITAL DATA AND ITS PROTECTION

[4]GobindVs StateofMP[(1975)2SCC 148
[5]RajagopalVs StateofTN[(1994)6SCC632]
[6] PUCL Vs UOI[(1997)1SCC301]

The EU directives established in the Guidelines establish individuals' rights and duties in the context of computerized personal information, as well as those who participate in such process. The Guidelines are applicable to personal information, whether it is in the publicly or privately sectors, that jeopardises privacy and rights of the individual due to how it is processed, its nature, or the context in which it is employed. The following are the OECD's core privacy principles**:**

Acquisition Restriction Concept: The acquisition of personal information must be limited, hence any information is needed lawfully and fairly, and, where applicable, with the knowledge or agreement of the data subject.

Personal data: It shall not be disclosed, made accessible, or otherwise used for purposes other than those indicated in line with [the Purpose Specification Principle] except: (a) with the data subject's agreement; or (b) by legal authority.

Personal data should be safeguarded by suitable security protections against threats such as loss or illegal access, destruction, use, manipulation, or disclosure.

Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Personal Involvement Doctrine: An person ought to have the jurisdiction to: a) procure verification from a relevant authority, or otherwise, whether or not the data processor seems to have information related to him; b) possess information pertaining to him conveyed to him within a reasonable time; at a reasonable charge.

International Concepts of Privacy

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

"Article 17 of International Covenant of Civil and Political Rights" (to which India is a party) states "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home and correspondence, nor to unlawful attacks on his honour and reputation"

"Article 8 of European Convention on Human Rights states" "Everyone has the right to respect for his private and family life, his home and his correspondence; there shall be no interference by a public authority except such as is in accordance with law and is necessary in a

democratic society in the interests of national security, public safety or the economic well-being of the country, for the protection of health or morals or for the protection of the rights and freedoms of others."

PRIVACY PRINCIPLES IN INDIA

In the recent years due to the various incidents of data theft and misuse of personal information by BPO employees have raised the need for a specific law on data protection and privacy.[7] The Government of India in 2005 proposed certain Amendments to the existing IT Act. The IT Amendment Bill, 2006 makes specific provision in relation to data protection and imposes high penalties. Through this amendment Indian Government has tried to bring the legal regime in consonance with the *"European Union Directive on data protection"*.

Thus in the wake of recent incidents of personal data misuse and abuse the "*Data Protection Law of 2006 was implemented. This bill was submitted in the RajyaSabha on December 8th, 2006, following in the footsteps of international laws."* The objective of this proposal is to safeguard an individual's info collected for a specific intent by one institution and to prevent its use for commercial or other reasons by another institution, as well as to entitle oneself to seek money or destruction of property due to disclosure of personal data or information of any person without his consent, and for matters connected with or incidental to the Act. This Act makes provision referring to the type of data to be gathered over a certain purpose as well as the volumes of information to be acquired for the that reason. Data controllers have been proposed to be appointed to investigate any violations of the proposed Act.

Privacy is guarded by tribunals utilizing implicit protections based on common law, equity principles, and also the legislation of fraudulent misrepresentation. The Supreme Court of India acknowledged the right to privacy as a basic right under "*Article 21 of the Constitution in a significant judgement delivered in August 2017 (Justice K.S Puttaswami& others Vs. Union of India), as part of the right to "life" and "personal liberty." "Informational privacy" has been acknowledged as a component of the right to privacy, and the court ruled that information about a person, as well as the ability to obtain such information, require privacy protection ("Privacy Judgment").*"

As a result, the Government of India established a committee to design a data protection act.

[7]For example, in June 2005, American business outsource and their Indian counterparts were extremely concernedwhen Interpol was asked to investigate allegations that a 24-year-old worker at *Infinity eSearch*, a web marketingcompany in New Delhi, had sold information that he obtained from call center workers at a BPO company. Anundercover British reporter from a London tabloid newspaper, *The Sun*, claimed that the Infinity e-Search employeesold him Barclay Bank account details for 1,000 U.K. customers. The account holders' secret passwords, addresses,phone numbers, and passport details were allegedly sold for 350,000 rupees (INR 350,000), which is the equivalentofaroundU.S.$8,000

The committee presented a draught law, and the Government of India published the *"Personal Data Protection Bill 2019 ("PDP Bill") based on the committee's proposal. This would be India's first data protection law, and it will remove Section 43A of the IT Act. The Bill's expected requirements are summarized here in brief."*

Entrance into force

"Sections 43A and 72A of the IT Act went into effect on October 27, 2009. The Rules went into effect on April 11, 2011. The Aadhaar Act went into effect on September 12, 2016."

CONCLUSION

There are various sectors that are engaged within the work of business method outsourcing and each sector has its peculiar demand concerning data protection. Thus a generalized overseas BPO legislation ought to be introduced as a result of data security is quite mere economic goods and demands a lot of protections than this utilitarian leveling affords. Watching data solely as having amount whole negates the idea of a right to private liberty and privacy incorporated all told the Constitution round the world. The commercialization of data ignores important personal worth placed on one's own privacy and ends up in a regime of under-protection. Therefore, so as to shield data legislation ought to establish a minimum level of protection to make sure that data isn't com-modified as an economically sensible and, therefore, isn't under-protected as such a good

[i] IT Act 2000