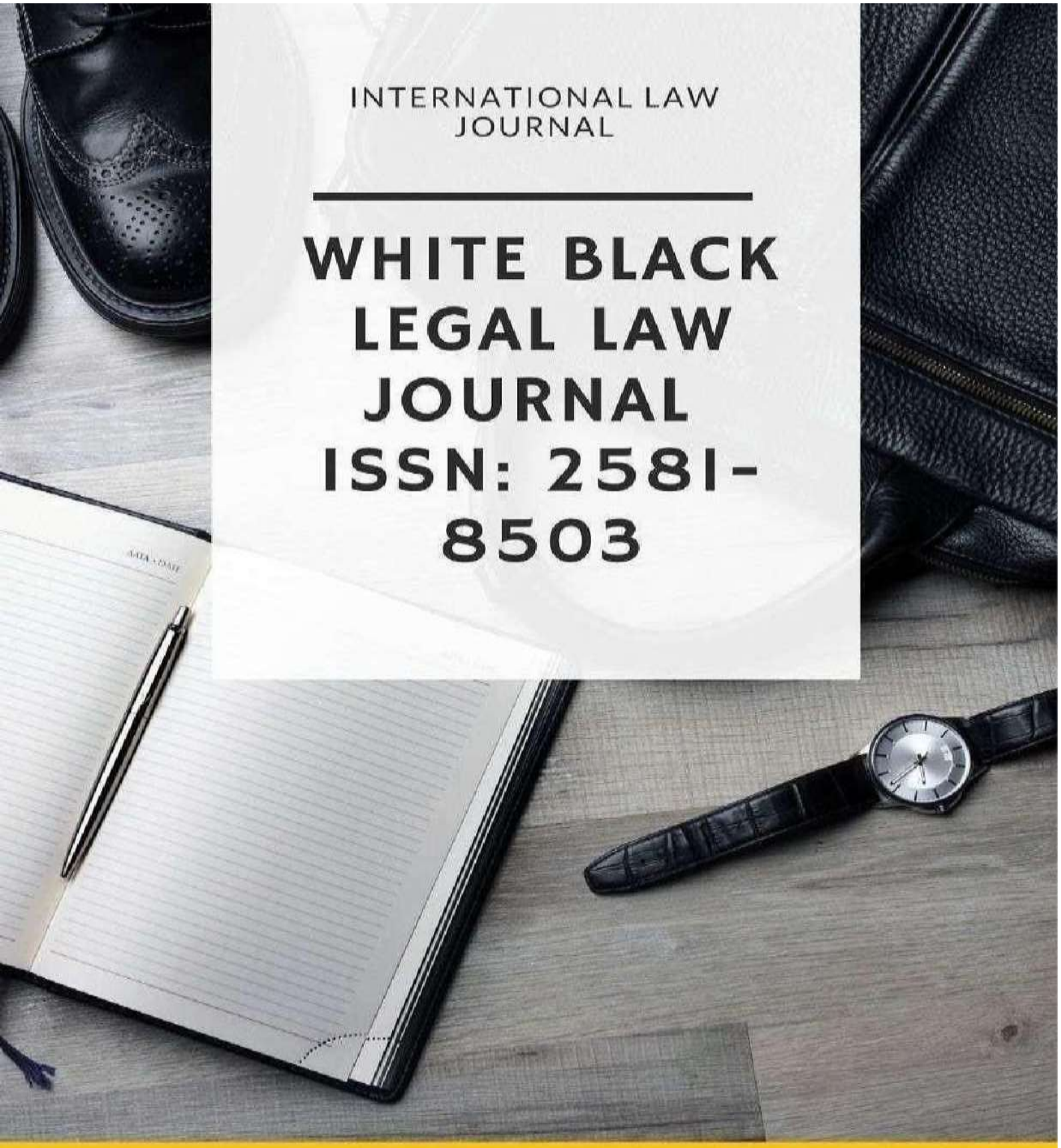

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

A STUDY TO UNDERSTAND THE LAW RELATING TO DATA PROTECTION OF COMPANIES

AUTHORED BY - PRATIBHA SINGH YADAV[1] & MS. RIDDHI TRIPATHI[2]

ABSTRACT

Information for knowledge based industry is like blood to the life of living beings. Information is worthy supplies not only for businesses like service and manufacturing, but adscititious it is perilous for economy and security of a nation. The utilization of data/information and its capability to get converted into progressive information is very paramount for businessmen, policymakers, scientists, engineers, etc. Having worthwhile and at times exclusive information can have betterment in productivity and quality which can advance the field of education, research and it supplemental benefits to make denizens more erudite.

Government's role in data security and ability to collect the private sector data is ambiguous in India. There are instances where the private sector provides data to government8 only upon a request, usually under any law, by-law, or under executive authority that enables the government to demand and collect this information. In India government has access to information held by the private sector. An example can be traditional search and seizure law, banking law, securities law and health law e.g. search and seizure law relevant provisions of law are Sec. 91 and Sec. 92 of Cr.P.C. government officials use these provisions to access information from private sector[3].

KEY WORDS: Data Protection, Company Etc.

INTRODUCTION

The last data protection bill, The Personal Data Protection Bill 2006, introduced in Parliament on 8 December 2006, has been lapsed. On 18 October 2010, the Department of Personnel and Training, Government of India, published an approach paper for legislation on privacy. The

[1] LL.M. (corporate law), Faculty Of Juridical Science Rama University, Kanpur.
[2] Associate professor, Faculty of Juridical Sciences, Rama University
[3] Richard A. Shweder & Edmund J. Bourne, Does the Concept of the Person Vary Cross-Culturally? Abstract visited at website on July 12th 2016

objective abaft this research was to examine the issues and challenges involved in protecting data. Rajeev Chandrashekhar, an MP came up with The Right To Privacy Bill at Rajya Sabha in February 2011. Protection to the privacy of a person including public figures was the main focus point of the Bill. While analysing the Bill, it seems that the bill focuses on safeguarding the use of electronic/digital recording devices in public spaces without consent rather than focusing on protecting individual's privacy. However, the bill had never passed If it was not for this rapidly increasing off-shoring business and the Unique Identification Number program, India would perhaps never have worried much about data protection, as there are already existing provisions in Indian licit framework for protection of data, though not at the scale at which protection is warranted under the current circumstances. The Aadhaar number, which is a single identifier of Indian citizen globally, is supposed to work across application domains which make individuals vulnerable to privacy breaches. In an Aadhaar like setup, the biggest threat to privacy emanates from potential insider leaks. The Aadhaar program does not seem to have been explicitly designed to have vigorous protections against such insider leaks. It seems that efficacious protection against insider leaks indispensably requires a data controller at UID headquarters as well as at the companies hired for the collection of data on behalf of the government. UID program has commenced and various complaints also have been registered against the company hired for accumulation of data by the government at several places. Thus, though there are earnest privacy concerns at present, we believe that Aadhaar can be made safe from the legal perspective by enacting a legal framework for data protection for concrete paramount reinforcing.

1.1 DEFINING THE TERM DATA

(a) Factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation or

(b) Information in digital form that can be transmitted or processed or

(c) Information output by a sensing device or organ that includes both useful and irrelevant or redundant information and must be processed to be meaningful."

In other words, data is any set of information that is collected, interpreted, and analysed for a particular purpose. When such data is represented using "machine language systems" which can further be construed by various technologies it is called digital data. In simple words, everything is data, right from emails, messages, phone calls, pictures, and videos, we post on social media platforms, to the purchases we make online, the places we visit, even the doctors

we see, medical reports, educational qualifications, the list can go on and on. A data trail is created by each time we are online. Today almost every technical device is becoming a source of data, which is becoming extremely valuable as the world continues to move in the direction of a data driven economy 'Information Economics'[4].

1.2 IMPORTANCE OF DATA PROTECTION

With data rising to become the most valued commodity today, organisations globally are focussing on ways for data protection to ensure unsanctioned access to sensitive information. Every organisation deals with an enormous amount of data daily which includes, customer information, product data, personnel company files, financial transaction data etc. Almost every decision regarding products and services, research and development is taken based on the data collected and stored by the companies. This makes data the most valuable asset of any organisation. Thus, to safeguard their most valuable asset, companies must invest in ways to protect it from falling into wrong hands. Since the advent of information technology and the world's complete reliance on computers in the past few decades business organisations as well as the government are amassing the personal data of people in their databases for reasons beneficial to them.

Each time a person uses the internet to buy or sell products, pay bills, or a matter of fact enjoys the fruits of social media he/ she gives away a vital part of himself/ herself in the form of personal information to these businesses. Without the knowledge of the users, their personal information is collected and often shared by companies as well as government agencies. Hence data protection applications supported by strong legislation are the only way to safeguard individuals from data misuse or abuse as well as corporate and state surveillance. The Facebook-Cambridge Analytica Scandal was an eye-opener for the world. It exhibited the capabilities of companies and the state to utilise the stored data for their personal, financial and political benefits. This is just the beginning, there may come a time when the technology could get out of hand as the human brain is capable of inventing wonderful things, computers being one. To safeguard ourselves and the future generation there is a dire need for regulating this exponentially growing technology. With a wide-reaching collection and transfer of data, there is an amplifying concern nationwide regarding the security of the personal data of individuals.

[4] Archana G. Gulati, Big Data-Competition & Consumer Protection Issues, Falling between Regulatory Stools?, in FORUM ON CHALLENGES OF COMPETITION IN THE DIGITAL ENVIRONMENT 2018 (2018).

Not only in India but the concern to protect data privacy is also being shared internationally. More so with expanding trans-border trade, possession of the maximum amount of data has proven to the highly beneficial to organisations. Thus, this gives rise to a key point to be taken care of while ensuring data privacy and data protection, and that is, the free flow of such data. Over-regularized data may prove to be a hindrance in the path of free trade practices. No country would like that keeping in mind how each nation is benefitting from free trade among themselves. Hence as data becomes the object of free trade, along with its positive usage it is also being exploited by organisations unethically to further enhance their profits. Recently people have become sceptical about giving away their data as they are not aware of who exactly is accessing their data. Is it protected enough not to fall in the wrong hands? Is it being used for the purpose their consent was taken for? Is there a possibility that such data may be potentially used to encroach on their fundamental rights? Thus, to ensure data security and win people's faith, data protection needs to be a paramount concern for both businesses and governments globally[5].

1.3 PRINCIPLES GUIDING DATA PROTECTION

The organisations (whether private or public) that are engaged in the activities of collection, storage or transfer of personal data of individuals are under an obligation to handle and safeguard such data according to data protection regulations. Understanding various international and national provisions regarding data protection one can summarize the following as data protection principles:

(A) Just, Unambiguous And Legal

Businesses and the State must focus on processing the personal data of individuals in a just, unambiguous and legal way. A just and unambiguous manner of processing is a requisite to ensure that personal data is in the way one expects it to be. Further, the processing of the personal data of individuals must be done in a lawful manner respecting the legislation in place for the same. The data owner must be made aware of the reason and ways in which his/ her data will be used by the data collector. In case the data collector intends to share or transfer the said data to any third party he must clearly inform the data owner about the same and take prior permission to do so. The presence of any sort of vagueness in this procedure makes it unfair

[5] What is Data Protection? - Definition from Techopedia, , TECHOPEDIA (2017), https://www.techopedia.com/definition/29406/data-protection (last visited Sept 21, 2021)

and tantamount to deceiving on the part of the data collector or data processor.

(B) Purpose Limitation

The purpose of the collection of data must be specified and strictly used for that purpose only. It is not acceptable and legitimate to later use the collected data for an unspecified purpose. If at any point the collector feels that the scope of purpose needs to be widened, additional consent for the new purpose of use of such data must be sorted. If for any reason the consent is not given the collector or processor must not use the collected data for any other purpose consent for which was not explicitly given. Apart from informing the data owner about the purpose for which the data is being collected the collector, or the processor must also identify its legitimacy i.e., all legal conditions must be identified and fulfilled. Purpose limitation is especially essential for businesses those profit from repurposing collected data. Such businesses must make sure that the personal data of individuals is not revealed or handed over for unspecified purposes and is processed according to the authority of law.

(C) Precision Of Data

Almost every business relies on data for policymaking decisions. This data must be accurate and recent for such businesses to flourish. If data is not duly updated and accurate businesses may end up with inaccurate decisions. It may on some occasions lead to the denial of services to individuals whose data is not accurate, complete or updated by the concerned department. For example, a person may be denied a loan as his credit score data is not accurate or not updated or incomplete.[6]

1.4 DATA PROTECTION AND RIGHT TO PRIVACY

Humans adore their privacy which distinguishes them from other animals. Privacy is a creation of mankind that has helped humans make remarkable scientific discoveries. As technology grew, it brought along with it many vices too. Yes, there is no doubt that technology has been a great help to mankind, but many found ways to use the same technology to violate other person's privacy. The invention of the printing press helped man to distribute his ideas easily, but it also encouraged some to reveal a person's personal writings. The invention of the camera gave rise to 'the fourth estate', the Press. But it also made the same press use this great invention

[6] Douglas Bonderud, What Is Data Protection and Why Does It Matter?, SECURITY INTELLIGENCE (2019), https://securityintelligence.com/articles/what-is-data-protection-and-why-does-it-matter/ (last visited Nov 16, 2021).

for wrong motives giving rise to yellow journalism. Postal and telegraphic services allowed us to send messages to our dear ones effortlessly, but they also made it easy for others to tap our personal messages.

Even though every time technology created wonderful things to make man's life easier and more comfortable, it kept taking away one of his precious belonging, his privacy bit by bit. The mention of privacy dates far back to 1604 in an English case, **Peter Semayne v Richard Gresham**[7] where the court specified how a representative of the State must approach and enter a person's house to issue warrants. However, it was for the first time in 1890 privacy was mentioned as a right by Warren and Brandeis in their timehonoured article "The Right to Privacy". This article is considered to be the holy grail for all privacy advocates even today. So much so that even the Indian Supreme Court, 2017 while pronouncing their judgment on the Puttaswamy case recognised the major role this article has played in the development of privacy laws around the world. Warren and Brandeis strongly advocated for the need for a law to safeguard the private space of an individual. They were extremely concerned with the advent of the camera and how the Press used it to intrude into people's personal lives. This article was later cited in many judgements by American courts and other courts around the world. The article was so impressive that even Roscoe Pound, an eminent legal scholar considered it to be a fresh chapter added to existing laws.

1.5 TYPES OF DATA

a) **Personal Data**: Any data that can be used to identify a particular person is considered to be personal data. In other words, 'identifiers' whether direct or indirect like name, address both home or work, email address, landline or mobile number, ID numbers or any other personal information are considered to be personal data. Often companies collect user personal data for business research and advertising purposes. Companies especially social media giants like Facebook collect and share user personal data with third parties. Based on users' likes, dislikes, online activities, web searches, online purchases, etc., these tech giants profile customer behaviour and bombard them with customised targeted advertising for their personal commercial gains. The topic of personal data and the legal issues surrounding it will be discussed elaborately in later chapters.

[7] 5 Co. Rep. 91a, 93a, 77 Eng. Rep. 194, 198 (K.B. 1604).

b) **Web Data**: Any data accessed either for a research study or otherwise is classified as web data. It may be government records, reports, business analysis, competitor information, any match score etc. It is productively used to monitor competitors, pursue prospective customers, shadow channel partners, create dominance, design apps and even more. Web data has the potential to convey insights and patterns about consumer likes, dislikes, needs, etc. and help companies understand their users much better. As the technology for converting unstructured data to structured data improves its usage will also enhance.

c) **Transactional Data**: Anything that requisites an act of collection be it an online purchase, visiting a web page of a company, clicking on a certain ad of a company, etc. is transactional data. Transactional data is collected by almost every website, either through, a third-party system, such as Google Analytics or any other internal data collection system, for progressive results. Analysing such data gives them an upper hand against competitors are they are better equipped with the correlations between patterns. Understanding these patterns businesses make better strategic and marketing decisions.

d) **Sensor Data**: Data produced by the smart things called the 'Internet of Things' (IoT) like a smartwatch, smart door locks, smart refrigerators, smart security systems, etc. is classified under sensor data. All these things connected to the internet enhance user experience and convenience creating related data each day and suggesting reforms to our daily routines. It allows endless connections between different connected devices by creating numerous opportunities for the collection of massive data by companies. One can say IoT are daily usage machines keeping a watch on us. The technology regarding IoT is still developing hence we need to understand the keep ourselves abreast with the issues and challenges surrounding this intrusive mechanization[8].

1.6 MEANING OF DATA BREACH

As per **Techopedia's definition**, "A data breach is an incident which involves the unauthorized or illegal viewing, access or retrieval of data by an individual, app, or service." When an unauthorised person or entity involves in the illegal access or retrieval of data from a system, network or company sites, with a motive to steal or publish such data elsewhere, it amounts to

[8] What is data, and why is it important? , IMPORT.IO (2018), https://www.import.io/post/what-is-dataand-why-is-it-important/ (last visited Jun 10, 2021).

a data breach. It may further be understood that when a hacker or malicious player unlawfully acquires personal, sensitive or classified financial information by gaining unauthorised access to a device or network system it is tantamount to a data breach on the part of such person. Inappropriate use of protected data directly or indirectly by cybercriminals for financial gains has seen a sudden rise in the past few years. 2018 was called the year of data breach by Malwarebytes Labs as the years saw the most cases of data breaches.

According to research conducted by Poneman Institute, the estimated price of a data breach incident worldwide in 2018 was "$3.86 million". According to an IBM report from July 2018 to April 2019, data breach incidents cost Indian businesses, at least Rs. 12.8 crore. The report emphasised that 51% of the data breach was due to malicious hacking, 27% was due to technical glitches and 22% of breaches happened due to human error. Personally identifiable information (PII), customer information, employee information, personal health information (PHI), credit/ debit card information, Aadhar card numbers, confidential company information, and intellectual property are some of the protected data or information which are directly or indirectly hacked by unlawful miscreants. However, all data breaches may not be intentional. On some occasions, protected data is mailed to the wrong address by mistake. A report published by Verizon in 2018 found that almost 17% of breaches took place by mistake. The report further found that even though sometimes data breach occurs due to mistake most of the breaches are intentional and for making quick financial gains. An IBM report covering the time period of May 2020 to March 2021 indicates a drastic increase in the incidents of data breaches during the pandemic which forced the entire world to stay at home and attend offices as well as school online[9].

1.7 TYPES OF DATA BREACHES

Distinct types of data breaches used by cybercriminals to acquire uninterrupted access to private information of a company, organisation or individual are as follows:

a) **Ransomware Attack**: This type of breach involves restricting authorised users to access their files by installing malware into their systems and insisting on paying a ransom in order to decrypt the files. It is a kind of digital blackmail that is the speediest

[9] What is a Data Breach?, TECHOPEDIA , https://www.techopedia.com/definition/13601/data-breach (last visited Jun 26, 2021).

challenge to cybersecurity and has approximately 2.8 billion distinct types that are identified to date.

b) **Phishing Attack**: When cybercriminals design apps, websites or even software that are a replica of the original apps, websites or software to deceive and extract personal information from individuals it is called a phishing attack. The replica is so convincing that people get conned and give away sensitive personal information like passwords, credit card numbers, and in a few cases even OTP.

c) **Malware Attack** When a hacker sends a link containing a virus including 'worms and trojans' in order to erase the entire system of the victim is called a malware attack. It is extremely damaging for companies whose entire work is based on data. For example, if hospital data gets erased by a malicious virus it may lead to very serious repercussions.

d) **Password Breach** Often people become victims of this type of breach, also known as a "brute-force attack" just because their passwords are too weak.39 Many people set their birth date or pet's name or baby's name or any other guessable passwords to their private systems. Such simple passwords are easy to guess and lead to data hacking smoothly. Sometimes the hacker designs a program that is capable of trying numerous passwords until it gains access to the targeted system or network.

e) **Keystrokes** Recording Another type of data breach is when a cybercriminal sends via email or inserts "malware called keyloggers" which are distinctively capable of recording everything one types on that computer or device. Such a breach can happen anywhere at the workplace or on a personal computer. The hacker gets access to all sensitive data on that device including passwords, credit card details, bank details etc[10].

1.8 LEGAL REMEDIES FOR DATA PROTECTION

With data becoming the most valuable asset, governments around the world need to regulate the collection, sharing and storage of the personal data of their citizens. Repercussions of a data breach can have profound consequences for not only individuals but businesses and governments too. As technology is evolving so are the kinds of crimes in cyberspace. Hence the law dealing with it cannot stand still and needs to evolve at an identical pace. The monopolistic approach of big data companies has created an imbalance in the existing relationship between data owners and data controllers. It is unfair for one sector to dominate

[10] Nikhil Arora and Darius Zinolabedini, supra note 63.

the other as the sustainability of an ecosystem suffers when disparity and inequality become this severe. In order to help data owners reclaim control over their personal data and demand more transparency on the part of the tech giants, in ways such as personal data is being used, governments around the world need to retrospect on how to regulate the activities of data controllers.

Any regulation about data protection must be balanced and mindful of the interests of all stakeholders vis-àvis private businesses, the public sector, tech firms and most importantly individuals. Many countries around the world have enacted their personal data protection regulations and are trying to do their bit in order to safeguard their citizens' personal data from any kind of misuse. Major corporations like Facebook and Google have been heftily fined for not complying with data protection laws of the land and forced to cough up millions of dollars for such breaches[11].

1.8.1 International Regulations

Not only the European Union, but many other countries have taken strong steps to regulate the menace of data breaches and have enacted or are close to enacting strict data protection regulations. Some of these enactments are as follows:

a) The General Data Protection Regulation (GDPR), 2018 – European Union
b) Personal Data Protection Act (PDPA), 2012 – Singapore
c) Lei Geral de Proteçao de Dados (LGPD), 2020 – Brazil
d) The Privacy Act, 1988 – Australia
e) Data Protection Act, 2018 – UK
f) California Consumer Privacy Act (CCPA), 2020 – California, USA
g) Protection of Personal Information Act (POPIA), 2020 – South Africa
h) Personal Data Protection Act (PDPA), 2019 – Thailand
i) Personal Data Protection Act (PDPA), 2010 – Malaysia
j) Protection of Personal Information (PPI), 2016 – Japan
k) Data Privacy Law, 2012 – Philippines
l) Personal Information Protection and Electronic Documents Act (PIPEDA) – Canada (Under review)

[11] Michel Kilzi, The Anatomy Of Personal Data Sovereignty, FORBES (2021), https://www.forbes.com/sites/forbesbusinesscouncil/2021/05/04/the-anatomy-of-personal-datasovereignty/amp/ (last visited Jul 8, 2021)

m) Personal Information Protection Law (PIPL), China

Apart from country-specific regulations, certain international organisations have also promulgated their data protection and data privacy guidelines to maintain international harmony and economic standards and encourage a smooth flow of international trade. These agencies are:

a) Organisation for Economic Co-operation and Development (OECD)
b) Asia-Pacific Economic Cooperation Forum (APEC)
c) United Nations Conference on Trade and Development (UNCTAD)

1.8.2 National Regulations

The Puttaswamy case (K.S. Puttaswamy v. Union of India) is a landmark decision by the Supreme Court of India in 2017, which recognized the right to privacy as a fundamental right under the Indian Constitution. While it primarily dealt with the question of whether privacy is a fundamental right, the judgment also had significant implications for data protection law in India. India has a sector-specific data protection regime. It was only after the Supreme Court declared the right to privacy an integral part of Article 21 of the Constitution of India in 2017 in the case of **Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors**[12], that the government constituted a committee in July 2017, under the chairmanship of retd. Justice B. N. Srikrishna to draft a data protection bill for the country. The committee submitted the Draft Personal Data Protection (PDP) Bill in July 2018, to the Ministry of Electronics and Information Technology. An amended version of this bill was presented in the Parliament in 2019 which was again amended and renamed as the Data Protection Bill, 2021. However, even this bill could not be passed, and the government drafted a fresh bill after withdrawing the 2021 bill altogether.

The new bill i.e., the Digital Data protection Bill, 2022 is yet to see the day of the light. Meanwhile, data is regulated by the following Acts in India:

a) Information Technology Act, 2000
b) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
c) National Cyber Security Policy of India, 2013
d) Draft Digital Information Security in Healthcare Act (DISHA), 2018

[12] (2017) 10 SCC 1.

e) The Aadhar Act, 2018
f) Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021
g) Personal Data Protection Bill, 2019
h) Digital Personal Data Protection Bill, 2022

CONCLUSION

India started liberalizing its economy from 1990 and since then a huge upsurge in the IT business process outsourcing may be witnessed. Financial, educational, legal, marketing, healthcare, telecommunication, banking etc are only some of the services being outsourced into India. This upsurge of outsourcing of ITES into India in the recent past may be attributed to the large English-speaking unemployed populace, cheap labour, enterprising and hardworking nature of the people etc. Statistics have shown that the outsourcing industry is one of the biggest sources of employment. In a span of four years, the number of people working in call centers in the country supporting international industries has risen from 42,000 to 3,50,000. Exports were worth $5.2 billion in 2004-2005 and are expected to grow over 40% this fiscal year. US is currently the biggest investor in Indian ITES, taking advantage of cheap labour costs. Statistics indicate that software engineers with two-year's experience in India are being paid about 1/5th of an equivalent US employee. With globalization and increasing BPO industry in India, protection of data warrants legislation.

There are reasons for this. Every individual consumer of the BPO Industry would expect different levels of privacy from the employees who handle personal data. But there have been situations in the recent past where employees or systems have given away the personal information of customers to third parties without prior consent. So other countries providing BPO business to India expect the Indian government and BPO organizations to take measures for data protection. Countries with data protection law have guidelines that call for data protection law in the country with whom they are transacting. For instance, in, the European Union countries according to the latest guidelines, they will cease to part with data, which are considered the subject matter of protection to any third country unless such other country has a similar law on data protection. One of the essential features of any data protection law would be to prevent the flow of data to noncomplying countries and such a provision when implemented may result in a loss of "Data Processing" business to some of the Indian

companies[13].

REFERENCES

1) Data Protection: A Practical Guide to UK and EU Law. by Peter Carey
2) Privacy and Data Protection in Business: Laws and Practice. by Jonathan I. Ezar.
3) Data Protection Principles in the Personal Data (Privacy) Ordinance. by Office of the Privacy Commissioner for Personal Data, Hong Kong.
4) Parag Diwan and Shammi Kapoor., Cyber and E-Commerce Laws with Information Technology Act,2000 & Rules therewith, Bharat Publishing House, New Delhi, 2nd Edition,2000.

[13] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Available at: www.whitehouse.gov .