Naveen Shodh Sansar (An International Refereed / Peer Review Multidisciplinary Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 8.054,
January to March 2025 E-Journal, Volume I, Issue XLIX, ISO 9001:2015 - E2024049304 (QMS)

Digital Data Protection and Artificial Intelligence: A New Era in the World

Deepika Joshi *

*Research Scholar (Computer Science and I.T.) Janardan Rai Nagar Rajasthan Vidyapeeth University, Udaipur (Raj.) INDIA

Abstract : The modern world is encountering new challenges, and the nature and forms of crime have transformed. Where earlier physical conflicts dominated criminal activities, today, online and digital platforms have taken their place. Most work is now conducted digitally. All government schemes are being provided online, which requires individuals to share their personal information. At the same time, the use of social media compels people to disclose much of their private information voluntarily. However, uploading personal data on social media always carries a risk of misuse. In the present times, digital data is considered the new gold, and the importance of data security is increasing globally. European countries have already implemented strict data protection laws. India is also advancing towards this direction. The introduction of artificial intelligence has brought a modern revolution that has significantly impacted various fields. Every sector is striving to make use of artificial intelligence, highlighting its importance in development. The primary objective of artificial intelligence is to make human life easier and to facilitate operations efficiently. This research paper will discuss the significance and need for digital data protection and how artificial intelligence plays a role in regulating it. It will also examine the current data protection laws and how artificial intelligence contributes to legal frameworks for data security.

Introduction - Human rights are not only necessary but also extremely important for an individual's independent and dignified way of life. Without them, one cannot even imagine living as a human being. If these rights include personal identity and biometric data, they become even more significant. The Universal Declaration of Human Rights (1948) under Articles 8, 12, 17, 18, 19, and 28 is associated with these rights. At the national level, Articles 19 and 21 of the Indian Constitution also pertain to such rights. The Supreme Court has elaborated on these rights through various judgments. In the Aadhaar card case, *Puttaswami (R) vs. Union of India* (2017) 10 SCC, privacy was declared a fundamental right. Human rights are ethical principles that establish certain standards of human behavior. These rights are recognized separately from national and international laws. They are considered "inalienable" rights, meaning they are inherent to humans from birth and remain with them even after death. They are not influenced by a person's age, place of residence, language, or other factors. In this era of modern technology, any individual's information can reach any corner of the world in an instant. A person's personal information may be misused, leading to violations of human and fundamental rights. The issue of data protection was raised in the Indian Parliament in September 2023.

Institution Made Stricter: The institution was made stricter, following the recommendations of the Krishna Committee. However, this issue becomes significant only when discussions about data collection are held for a limited period. However, human rights organizations do not consider it a violation, as the European Union has already established a special law for data collection. Hence, it is seen as a necessary process, but its implementation remains incomplete. India is one of the 27 countries worldwide where individuals are considered guilty of data theft and misuse. The collection of personal data in India is included in the list of potentially harmful activities.

Since the year 2000, information technology has been made stricter, which has led to increased cyber security measures over the last few years. However, business activities related to data protection have not been fully regulated. The Indian government passed the **Personal Data Protection Bill 2023**, which includes regulations on listening to personal data. However, the law is still unclear on some aspects and does not entirely prohibit violations of human rights.

European Union's Data Protection Regulation Law 2016:

1. This law will create new international standards, particularly for the protection of online information on platforms such as Facebook, and will address data

breaches.
2. Due to this new law, the European Union will once again establish control over its data.
3. The European Union has imposed penalties of up to 20 million euro's (24 million dollars) or 4% of the company's annual global revenue for data misuse by companies.
4. This law legally ensures that individuals must be clearly informed about how their data will be used and must give their consent for its usage.

Statistics: The **Constitution of Human Rights** in Article 3 recognizes the importance of digital data protection, aligning with the **Universal Declaration of Human Rights in 1948**.

1. When rights are linked to personal digital data, they become as crucial as the right to property in a traditional sense.
2. With the advent of modern technologies, digital data has become extremely valuable today.
3. Compared to European countries, India lacks stringent digital data laws, leading to increased violations of privacy rights.
4. According to NCRB data (December 2023), 65,893 cybercrimes were registered in India in 2022, marking a 24.4% increase compared to 2021.
5. According to IBM cyber security reports, on average, a cybercrime occurs every 39 seconds, affecting around 2,200 people globally.
6. The Cyber Security Annual Report 2023 highlights an increase in the number of phishing incidents in the Netherlands.
7. Data security issues were not addressed in educational policies.
8. In 2021, the Indian government failed to implement a national cyber security framework.
9. In 2021, there were 7,867 data breaches in India.
10. India lacks a well-established policy on data collection and its use.

Significant Decline in Data Protection: Major data breaches in the world:

1. The largest attack in Paris
2. Inadequate data protection laws - European Union, Iceland
3. Lack of data protection laws - Malaysia, Nauru

Other Countries' Laws:

1. GDPR (General Data Protection Regulation) is the data and privacy protection law of the European Union.
2. It holds a rightful place in human rights concerning data privacy issues.
3. It regulates the collection and use of personal data.
4. It mandates the security of stored data.
5. It allows individuals to control their personal data.
6. It gives people the right to amend and update their information.
7. It provides legal provisions for the excessive collection and misuse of data.
8. In 2020, Article 30 of the GDPR gave rise to the "Right to be forgotten".

USA

1. The USA does not have a uniform federal data privacy law, but it does cover health data, financial data, etc.

Switzerland

1. The data law guarantees the right to privacy.
2. Data processing without an individual's consent is restricted.

Britain

1. The Cyber Crime Act is the strictest in the world.
2. Storing any person's computer information illegally can result in 6 months in jail and a £70 fine.
3. Unauthorized data usage is a criminal offense.

Canada

1. Data must be stored in an encrypted form.
2. It is necessary to report if data is lost or leaked.

Importance of Data Ethics

Aspect	Description
Consent	Information Confidentiality
Security	Data Processing
Citizen Rights	Commercialization
Web User Assistance	Sending Commercial Messages

Key Points of the Personal Data Protection Act, 2003

1. This law applies to the storage of personal digital data.
2. The user must be informed about how their data will be used. If the data is transferred to goods or services outside India, consent is required.
3. Special permission is needed for processing sensitive data, and it should not be used for unauthorized purposes.
4. Organizations must keep personal data accurate, secure, and up-to-date, and delete data once the purpose is fulfilled.
5. Individuals have the right to access, modify, and delete their personal data.
6. If data privacy is violated, legal action can be taken.

Artificial Intelligence (AI): Artificial intelligence is a branch of computer science focused on developing systems that can simulate human cognitive abilities. AI is currently being used in various fields such as education, healthcare, telecommunications, and automation. Many other industries are also adopting AI-based solutions.

AI is classified into the following types:

1. **Specialized Artificial Intelligence**
2. **General Artificial Intelligence**
3. **Human-like Artificial Intelligence**

AI emerged as an academic discipline in the 1950s. Between 1970 and 1975, research in AI led to many significant developments. In the 21st century, AI has become an integral part of digital technology. In 1956, the AI sector was formally established.

The Prime Minister has emphasized India's participation in AI-driven solutions, highlighting its role in

economic growth. The first global summit on AI was held in India on October 29. With the rise of AI, discussions on ethical considerations have also emerged. Ethical AI usage is necessary to prevent harm. Governments worldwide are setting policies to regulate AI applications. AI should be implemented responsibly to avoid misuse.

In 2020, the Indian Data Security Council was established. In the report presented by this council, several government initiatives have been mentioned to ensure a secure, reliable, scalable, and safe cyber space in India. These initiatives in the direction of "Cyber Security by Data Security" include:

1. Cyber Security India Initiative
2. Cyber Hygiene Center
3. National Cyber Crime Reporting Portal
4. Indian Cyber Abuse Reporting Center
5. Information Technology Act 2000
6. Digital Data Act 2023

Conclusion: The government can issue such guidelines for individuals and private organizations that ensure the protection of information infrastructure and keep the process of data protection in place. It should implement such standards that align cyber users' roles with moral integrity and legal framework, preventing potential legal violations and ensuring ethical leadership in society.

References:-

1. Competitive Review / January 2024, 103
2. Civic Cyber Links / June 2022, 27
3. Indian Cyber Security Council - Manuscript
4. Secure Cyber Infrastructure - Policy Framework
5. Information Technology Act 2000 (Government of India)
6. Personal Digital Data Act - Gazette (Government of India)

✻✻✻✻✻✻✻✻✻✻✻✻