# LEGAL & ETHICAL SAFEGUARD FOR DATA PROTECTION, CYBERSECURITY AND AI GOVERNANCE

*By Utkarsh Mishra[*] & Simran Bundela[**]*

**ABSTRACT**

*Technology in this rapid world changing rapidly. It has numerous opportunities for this generation, but those who use it without care and caution and gives the information to any site knowingly or unknowingly. Such negligence gives hackers a chance to acquire information and abuse it against an individual or organisation to rob cash or blackmail users. The matter of privacy and security of personal information and data has now attained a precarious point due to carelessness. The government should address requirements in order to ensure safe and ethical use of data. The governments can protect our action by merely simply change and modification in the laws about fair and ethical use of data. This can be achieved through reformed laws or establishing new laws pegged on the activities of how data may be gathered and utilized by the sites and companies. All these can be implemented with the legislations that governs the ecosystem whereby both extremes can be both legal and ethical. Therefore, in this paper, we will elaborate on how the government must put in place to assure legal and ethical applications of AI, Data Protection and Cybersecurity to make sure that all norms are collaboratively put to guard individual rights and obligations.*

**Keywords**: Cybersecurity, Law, Ethical, Attack, Personal Data, Protection, Government, Privacy.



[*] 3rd Year, LL.B. (Hons.) 5 Year Degree Course, University of Lucknow. Email- utkarshmishraindia@gmail.com.
[**] 3rd Year, LL.B. (Hons.) 5 Year Degree Course, University of Lucknow. Email- simranbundela877@gmail.com.

## I. Introduction

Transformation, in a basic sense, can be a change over time to be useful and meaningful throughout the time. The transformation is necessary to keep things working. Technology also has a significant role in the society, in terms of transformation and has drastically changed various aspects of the society including healthcare, education, finance, governance and etc, and some of the study indicate that 2.5 quintillion bytes of data are generated every day[1]. And the pace of the transfer of data is sufficient to demonstrate colossal possibilities of innovation and sustainable development. And due to such ample usage of data, it turned prone to cyberattack, privacy breach, digital profiling and unethical data usage.[2]

The government in such atmosphere where data use is so much, yet, the means of security are fewer, should do some steps and these must be resilient, adaptive and be ethically the right thing to do. As, Inida earlier govern these practices through Information Technology Act, 2000[3]. Under section 43[4] and section 66[5] imposes the punishment and compensation for the damage caused and for illegal action done by the or to the computer system. And also section 72A[6] provide penalty for breach of confidentiality and privacy. Although the act is not that effective as its basic aim towards technology oriented, but it laid down the foundation for data protection and cybersecurity as legal obligation. Therefore, the government should be more resilient to deal with the risk, continuity, and to assist in developing legal and ethical standards. As the theme of this article was the "Resilient Leadership of Sustainable Growth." This means that the government should consider AI Governance, Data Protection, and Cybersecurity frameworks in its decision-making processes.[7]



Since the abstract is targeted at the user and organisations that tend to act irresponsibly and disclose sensitive data, disregard the cybersecurity rules, and do not adhere to the ethical standards of data use. Such carelessness creates criminals. The government ought to do this so

[1] Marr, B. *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Rea*d https://bernardmarr.com/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/
[2] Aswathy, S.U., and Tyagi, A.K. (2022). Privacy Breach through *Cyber Vulnerabilities: Critical Issues, Open Challenges, and Possible Countermeasures for the Future, in Security and Privacy-Pressing Techniques in Wireless Robotics* (1st ed.). CRC Press 2022.
[3] Information Technology Act, 2000 (India).
[4] Information Technology Act, 2000, Section 43 (India).
[5] Information Technology Act, 2000, Section 66 (India).
[6] Information Technology Act, 2000, Section 77A (India).
[7] Chelvachandran, N., et al. (2020) Considerations for the Governance of AI and Government Legislative Frameworks," in H. Jahankhani, S. Kendzierskyj, et al. (eds.), *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity* (pp. 57–69). Springer International Publishing, Cham, 2020.

that organisations and users ought to abide by legal frameworks, and the government ought also to ensure that these frameworks are updated frequently.

## II. AI Governance and the Need for Ethical Leadership

### A. *Growth of AI and Government Responsibilities:*

AI most intelligent tool ever built by humanity, which influences how decisions across the world. Governments increasingly relies on AI systems for efficiency and competitive advantage. According to Stanford's Global AI Vibrancy Ranking 2023[8] research mentions that the United States is a global leader in AI, excelling in research, private investment and advanced AI models. Companies like Google, OpenAI, Microsoft and NVIDIA drive major AI breakthroughs. After USA, China is on 2nd, UK on 3rd and India on 4th as per their ranking. However, if the AI is not properly monitored by the governments, it has risk of becoming biased, opaque and environmentally harmful, etc.[9] Governments in this situation should focus on how to make AI free from these problems as the OECD Principles on Artificial Intelligence (2019)[10] and UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)[11] suggested comprehensive approaches for the countries to fix accountability, make AI deployment fair and transparency and human oversight. Also, According to Pew Research Centre[12], they mentioned three steps the government should take to remove these negative, biased and opaque data's these are:

- Firstly, they emphasize the global cooperation of AI development that requires a common and international understanding and a unified approach to creating cohesive strategies and policy making. It makes states agree on fundamental principles and regulations for AI to ensure it benefits people at large.



[8] Fattorini, L., Maslej, N., Perrault, R., Parli, V., Etchemendy, J., Shoham, Y., & Ligett, K. (2024, November). *The Global AI Vibrancy Tool.* Institute for Human Centered AI, Stanford University. available at: https://hai.stanford.edu/assets/files/global_ai_vibrancy_tool_paper_november2024.pdf

[9] IBM, (2024). *10 AI Dangers and Risks and How to Manage Them*. https://www.ibm.com/think/insights/10-ai-dangers-and-risks-and-how-to-manage-them

[10] Organisation for Economic Co-operation and Development. (2019). *What Are the OECD Principles on AI?* https://www.oecd.org/content/dam/oecd/en/publications/reports/2029/06/what-are-the-oecd-priciples-on-ai_f5a9a903/6ff2a1c4-en.pdf

[11] United Nations Educations, Scientific and Cultural Organization. (2021). *Recommendation on the Ethics of Artificial Intelligence.* https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence

[12] Anderson, J., & Rainie, L. (2018, December 10). *Solutions to address AI's anticipated negative impacts.* Pew Research Center. https://www.pewresearch.org/internet/2018/12/10/solutions-to-address-ais-anticipated-negative-impacts/

- Secondly, call for creation of specific policies and regulations that ensure that the AI are designed to enhance and assist humans, and focuses on achieving the common good rather than replacing humans.
- Thirdly, it focuses on systematic societal change that empowers people by reforming the field of economic, political and educational systems.

These are some criteria suggested in the research that the government took to resolve the problems of AI exploitation and injustice.

B. *Ethical Dilemmas in AI Deployment:*

According to the USC Annenberg Centre for Public Relations Report[13], it highlights several key challenges and concerns related to the development and deployment of AI. It was divided in two major categories:

1. Core Ethical Issue in AI Development

- Bias and Fairness: AI system often provide biased results that they inherit from the organisation that they were developed by which leads to unfair and discriminatory results.
- Privacy: The system requires a vast amount of data processing to provide the result, therefore, while providing the result to the user, AI sometimes provide the data that was of a private nature.
- Control: AI day by day becoming more and more self-reliant as technology advances, it raises the potential loss of human control over it. It is very concerning as AI is also used in military, medical, engineering, etc. which sometimes have life and death on the stake.



These ethical concerns are interpreted in the case of **Justice K.S. Puttaswamy v. Union of India (2017)[14]**, where SC recognised the Right to Privacy as a fundamental right under Article 21 of the Constitution[15] and by which it compels government to regulate the AI and frame laws and policies to protect right of the people.

[13] USC Annenberg Center for Public Relations. (n.d.). The Ethical Dilemmas of AI. http://annenberg.usc.edu/research/center-public-relations/usc-annenberg-relevance-report/ethical-dilemmas-ai
[14] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[15] Constitution of India. (1950). Article 21.

2. Societal and Economic Impacts

- Job Displacement: AI is starting to take various work from humans as they are more economical and provide better and fast results compared to humans, which directly leads to job loss and increasing economic disparity.
- Environmental Impact: As AI consume a large amount of energy to run, it requires large amount of raw material and water to run efficiently and also produces large amount of electronic waste that includes hazardous material such as mercury and lead that damage the environment at its worst.[16]

## III. Data Protection a Strategic Imperative

### A. *Rise of Data as the New Currency*

Data a highly valuable and influential asset that drive economics. It works as a foundation for the digital economy that powers AI. Like a traditional currency, the value of data also depends on its flow, verification and security. An estimated 25 billion devices are connected by 2020, because of this massive number, it largely impacts the business and society. Such as[17]:

- Because of the large amount of the data, it helps businesses to exactly tell the customer what they want and where they can get it.
- In a survey[18] it was cited that company's revenue is significantly increased when they invest in a system to manage the data efficiently which has the ability to better understand their customers.

We can say now that data is becoming the new source of wealth and value in the digital economy, which has an enormous potential and offers many opportunities to societies and companies to transform and also provide responsibilities to the leaders and policymakers is to est. the necessary frameworks to guard it.

### B. *Threats Emerging from Poor Data Practice*

Poor data Practice has created significant threat of a data breach, which can result in financial loss and legal penalties and also cause extensive reputational damage. Such issues arise only

[16] United Nations Environment Programme. (2025). *AI Has an Environmental Problem: Here's What the World Can Do About That.* https://www.unep.org/news-and-stories/story/ai-has-environmental-problem-heres-what-world-can-do-about

[17] World Economic Forum. (2015). *Is data the new currency?* https://www.weforum.org/stories/2015/08/is-data-the-new-currency/

[18] Tata Consultancy Services. (2025). *Internet Of Things: TCS Global Trend Study 2015*. https://www.tcs.com/who-we-are/newsroom/press-release/iot-tcs-global-trend-study-2015

when the security for data protection is not sufficient, the data is of low quality and a poor policy framework. Some of the threats are:

- Cyberattacks: The cybercriminal can actively exploit the weak data protection that is guarding it and it can easily demand the money for it or can easily reveal the sensitive data out.
- Leakage of Personal Information: Data breach can easily access the sensitive information which can include phone no., financial record, health record or even passwords.
- Financial Fraud: Attacker after gaining info about bank details, relevant documents, and passwords can perform various fraudulent exercises such as making fraudulent transactions, opening a new bank account in the victim's name and misuse the credit card, etc.
- National Security Risk: When sensitive details of the country are compromised, and the strategic data falls into foreign hands, it can risk the national security because of the poor data management.

C. *Legal Frameworks Ensuring Data Protection*

The primary legal framework that protects data in India is the Digital Personal Data Protection (DPDP) Act, 2023[19]. In India it establishes a comprehensive law for protecting the digital personal data by defining the right of individuals whether they are users or organisations. It focuses on consent of the users, purpose limitation and accountability of the users and the organisations. This framework is supported by earlier legislation, like the Information Technology (IT) Act, 2000[20] and the Court's rulings it is also similar to European Union's General Data Protection Regulation (GDPR)[21]. The World Bank's Identification for Development Guide[22] has outlined various essential policy frameworks for the protection and privacy of the data. These legal frameworks are:

- Institutional Oversight: There will be a supervisory authority that is independent from influence and regulate the flow of the data. This authority must be purely independent

[19] Digital Personal Data Protection (DPDP) Act, 2023 (India).
[20] Supra 3.
[21] GDPR.eu. (n.d.). *What is GDPR?* https://gdpr.eu/what-is-gdpr/
[22] World Bank. (n.d.). *Data protection and privacy laws.* https://id4d.worldbank.org/guide/data-protection-and-privacy-laws

which means that its appointment, its composition and its power to make decisions are not affected by external interference.

- Data Security: Data should be stored such that it is processed securely and protected against unauthorised and unlawful practices. Data properly encrypted, anonymised, and the system should ensure proper confidentiality and integrity with the system that has the ability to restore data after a physical and technical incident.
- Cross Border Data Transfer: Data transferring from one nation to another should follow major international standards. The countries should limit the extraterritorial transfer of personal data to foreign countries unless the country has an adequate level of protection.
- User Consent and Control: Transparent disclosure of what personal data is being collected and how it will be used. The legal framework must guarantee the right to data to the users and their data must be used for a useful purpose and companies without users' consent cannot transfer or disclose the data to any other person or organisation for the purpose of profit. But, in exceptional cases data can be shown to the government when the topic is of national security and integrity.

## IV. Cybersecurity as the Foundation of Digital Resilience

### A. *Understanding Cybersecurity within Leadership*

Cybersecurity is most of the time considered as the technical function rather than focusing on its legal aspect to protect the data. Now in a new digital age, where data works as a digital currency it has now become the central pillar for digital economy therefore, the leadership should take responsibility. Leadership should understand that cybersecurity is fundamentally about protecting people rights rather than viewing it as a technical or cost burden. Leadership must also anticipate risks and react to them proactively like identifying emerging cyber threats, allocating resources for prevention and ensuring continuous monitoring. Lastly, government under CERT-In Direction, 2022[23] make organisation and companies to follows its norms and reports cybercrime as early as possible and also make them responsible.

### B. *Types of Cybersecurity Threats Leadership Must Address*

There are various cyber threats that leadership must address to resolve the problem. These are:

[23] CERT-In. (2022). *Directions under sub-section (6) of Section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents.* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

1. Malware: It is also known as Malicious Software it was intentionally made to harm a computer system. Now, modern cyberattacks most of the time use some type of malware software for gaining unauthorised access to the device so to destroy, steal or leak the data stored. These are of various types[24]:
   a. Ransomware: In this type of attack, attacker locks a user data or a device and threatens to leak it unless some amount is paid to them.
   b. Trojan Horse: These malicious programs are appeared to be a useful tool to trick people to download the software and when they successfully install it, the software starts performing its malicious tasks such as stealing sensitive data, installing other malware, etc.
   c. Worms: It is self-replicating programs that automatically spread to application and device without any human interaction.
2. Phishing: It is also known as *"Human Hacking"* which means that it influences the person through a fraudulent message or phone call which leads to exposing the confidential information or compromise the security.
3. Denial of Service (DDoS) Attack: In DDoS attackers make online service unavailable by overwhelming them with excessive traffic from various location and sources. It is often used to shut down large network sites.
4. Corporate Account Takeover (CATO)[25]: It is a business entity theft where attackers impersonate the companies to send unauthorised wire and ACH transactions to account, they control through this the attacker tries to infect the computer to gain access to the banking system and can easily target for high loss crime.



These are the some most known cybersecurity threats. There are still many other types of cyber threat such as Zero Day Exploits, Password Attacks, IoT Attack, and ATM Attack.

### C. *Human Behaviour and Ethical Responsibility in Cybersecurity*

Cybersecurity does not solely depend upon technology it is equally and sometimes more depends upon human behaviour. In a Research Paper titled "Human Behaviour and Cyber Security: Bridging the Gap Between Technology and Psychology"[26] they have surveyed 100 people from 18 years to 30 years and gathered the data on their security mindfulness and

[24] IBM. (2024). *Types of Cyberthreats*. https://www.ibm.com/think/topics/cyberthreats-types
[25] Massachusetts Office of Consumer Affairs and Business Regulations. (n.d.). *Know the types of cyber threats.* https://www.mass.gov/info-details/know-the-types-of-cyber-threats
[26] Poojari, D., & Mhatre, G. (2023). *Human Behaviour and Cyber Security: Bridging the Gap Between Technology and Psychology.* Journal of Emerging Technologies and Innovative Research (JETIR), Vol. 10, Issue 12.

behaviour. And, out of which 76% of the people believed that human behaviour plays a significant role in cyber security incidents.[27] 88% also believe that perceived psychology can play an important role to enhance cybersecurity measures.[28] And, in one of the studies shown that 85%[29] of Successful cyber-attacks involve a human element. So, the government must take the matter as an ethical responsibility and start an awareness program, regular training sessions, try to develop accountability mechanisms and do other practices that help people to become aware. Leadership should also demonstrate ethical behaviour themselves by using secure platforms, avoid shortcut methods and setting a standard of the work. It is also the responsibility of the users to that they must check before logging at any site that it's secure or not and they should also avoid downloading from any known site. Through these acts, a strong ethical foundation will be built upon all levels with a shared responsibility

## V. The Role of Government in Legal and Ethical Safeguarding

### A. *The Need for Timely Legislative Reforms*

Structural and functional reforms are required to account for the changing economic and social environment. Legislative reforms may lead to outdated laws that do not meet the contemporary needs of the modern world. Lack of reforms may lead to decline and weakening of democratic governance, a government undergoes structural and functional reforms in order to stay effective and accountable. Such as[30],

- Need for stronger legislative scrutiny, to ensure better planning and drafting of the laws and by ensuring that the committee reports are debated in the house.
- An enhanced financial oversight that reforms the budget making process so that it aligns with modern economic needs and by including stronger mechanisms for parliamentary control over government borrowing and spending.
- Improving the parliament's image and effectiveness by rebuilding public trust and improving the image of the Parliament, by raising the quality of the performance of the MPs and also by cutting unnecessary expenditures in the parliamentary functioning.



[27] Supra 26
[28] Ibid
[29] Verizon Business. (2021). *2021 Data Breach Investigation Report.* Verizon.
[30] Ministry of Law and Justice, Government of India. (2002). *Working of Parliament and Need for Reforms* (Report of the National Commission to Review the Working of the Constitution, Vol. 3: Consultation Papers).

- Procedural and structural changes are also required such as reforming the ways in which the parliamentary parties' function by adopting different procedural improvements and making the functioning much smoother and efficient.

The three key reforms which are needed to fix the poor functioning due to the delays and weak accountability are[31];

- PM Question Hours: Dedicated sessions where the MPs can directly question the PM regarding national and cross-ministry issues.
- Accountability of Regulators: the regulators exercising major executive powers like the SEBI, TRAI, FSSSAI should all be answerable to the parliament for holding accountability.
- Stronger Committee System: For ensuring proper scrutiny of the policies and decisions by ministers in parliamentary committees.

B. *Balancing Innovation and Regulation*

The evolvement of technology at a fast pace is significantly impacting the economy, society and law in absence of proper governance. The risks such as privacy concerns, inequality, cybersecurity threats and environmental harms are overshadowing its' benefits. The innovation has outpaced the legal framework i.e. the pace of innovations is exceeding the pace at which laws and regulations can be developed and adapted.

Traditional legal systems are rendered unable to identify the unique risks and threats such as algorithm bias, lack of transparency, data and privacy threats and unclear accountability which are posed by the generative A.I. To navigate this complexity, there is a need for a harmonising legal framework to balance innovation and its governance. These can be[32]:

- Leveraging Existing Frameworks: The existing laws on data privacy, consumer protection and intellectual property should be updated and adapted to address the A.I. related challenges without stifling innovation.

[31] Sonu, D. (n.d.). Strengthening the Indian Judiciary: Comprehensive reforms to reduce delays and ensure timely justice.
[32] World Economic Forum. (2024). *How to balance innovation and governance in the age of AI.* https://www.weforum.org/stories/2024/11/balancing-innovation-and-governance-in-the-age-of-ai/

- Multistakeholder collaboration: Multistake-holder approach including the government, civil society, industries, academia to encourage transparent and ethical practices and development of A.I.
- Preparing for Rapid Evolution: Creating an agile and forward-looking governance in order to handle the rapid technological advancement i.e. developing foresight mechanisms to mitigate future risks. It includes conducting impact assessment and collaborating with International Organizations to align regulatory standards globally.

C. *Public Awareness and Digital Literacy*

One may refer to this as Digital Literacy, which is the ability to use online digital devices and services in our day to day activities. It is also aimed at empowering the individuals and laborers with rudimentary ICT skills in showing the livelihoods and accessing state services and participate in democracy. The services that are cheaper and more accessible become more transparent and, in turn, more open, which improves the health, education, employment and enables the social and cultural mobility and can impact the socio-economic development of the country. It is linked with the risk of cyber security which requires the users to save their information and avoid any transfer of sensitive information. India boasts of approximately 38 percent household digitization levels.[33] There is a wide gap in rural-urban gap. The urban salaried workers have the highest 68% of digital literacy[34] while the rural agricultural workers and Scheduled Tribes have the lowest digital literacy of 25%.[35] The fact that the digital literacy levels are generally low makes the threats and cyber-crimes more likely. These problems include phishing, OTP frauds, fake apps, and identity theft frauds, though the former and rural users are the main target.[36] To overcome this difficulty, it may be suggested to integrate cyber security into school and college schedules and create a proper content with assistance of content base training. The digital frauds must be introduced to the general population especially the population in rural areas through adverts and campaigns and made more aware by adverts and awareness programs by the government or the people themselves in partnership with a partner.

[33] Dattopant Thengadi National Board for Workers Education & Development, Ministry of Labour & Employment, Government of India. (n.d.). Digital Literacy https://dtnbwed.cbwe.gov.in/image/upload/Digital-Lieracy_3ZNK.pdf
[34] Supra 30
[35] Ibid
[36] Kumar, S., & Bansal, G. (2025). Cybersecurity awareness and digital literacy in the context of digital India. International Journal of Applied Research, 11, 434–439.

All these various efforts can be integrated to increase cybersecurity awareness, including digital literacy.

## VI. Conclusion

The fast change in technologies has rendered AI, Data Protection and Cybersecurity the key to growth and powerful leadership. Along with that, when these technologies introduce novelty, it also introduces certain grave threats that include privacy invasion, cyberattack, discrimination in the AI system that inevitably caused a gap of trust. They need to be managed by AI to provide transparency, accountability and human oversight, which complies with constitutional values of Right to Life and Personal Liberty in Section 21[37].

As, Data over the year emerged as a critical economic asset, requiring strong legal safeguards to prevent misuse of technology. India's Digital Personal Data Protection Act, 2023[38] represents a significant step and also recent enactment of Bharatiya Nyaya Sanhita, 2023[39] and Bhartiya Nagarik Suraksha Sanhita, 2023[40] reflect government steps to modernise the Indian Criminal Laws. Since Digital Personal Data Protection Act, 2023[41] are guaranteed by the right to forgotten, companies must obtain consent prior to the utilization of information as well as fixes accountability. And, cybersecurity should appear as a legal and ethical concern instead of technical elements since most of the cyber crime contains human behaviour as a contributing factor. Finally, the challenge of resilient leadership demands the right based legal framework in facilitating ethical leadership and knowledgeable citizens since this is the only way to attain a secure, inclusive and sustainable digital future.



*******

[37] Supra 15
[38] Supra 19
[39] Bharatiya Nyaya Sanhita, 2023 (India).
[40] Bharatiya Nagarik Suraksha Sanhita, 2023 (India).
[41] Supra 19