Page 4079 - 4091 **DOI:** *https://doij.org/10.10000/IJLMH.119449*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Traversing AI, Governance, and Privacy Laws: The Legal Divide in Democracy and Autocracies

VANSHIKA JAIN[1]

ABSTRACT

AI is a mirror, reflecting not only our intellect, but our values and fears." The rapid advancement of Artificial Intelligence technology and its integration in our day to day lives presents unique challenges to the privacy and data protection of individuals and organizations, making it a central concern in legislative debates around the globe. With UDHR declaring Right to Privacy as a Human right, and the launch of Privacy Guidelines by Organisation for Economic cooperation, and Development (OECD)and United Nations Sustainable Development Group (UNSDG), to ensure data privacy and free flow of Data across borders, it became essential for countries to ensure that they are protecting the Privacy of their citizens in line with these International Mandates. The paper aims to analyze how countries with different governance regime i.e. Authoritarian vis. Democratic, approach the governance of Data Privacy in today's age of Artificial Intelligence and whether or not these regulations are in line with the global standards of privacy as setup by OECD, and UNSTG. By comparing data protection regulations of these countries such as General Data Protection Regulation (GDPR), 2016 of Europe, Digital Personal Data Protection Act (DPDP), 2022 of India, and the Algorithmic Accountability Act, 2023 of USA with Personal Information Data Protection Regulation (PIPL), 2021 of China, Russian Federal Law on Data Protection, 2006, and Personal Data Protection Law (PDPL), 2023 of Saudi Arabia, the paper highlights the impact of governance regime of these countries on their approach to privacy regulation. Ultimately, the paper underscores the need for effective data privacy regulation to safeguard fundamental rights in diverse political landscapes.

***Keywords**: Artificial Intelligence (AI), Governance, Data Protection, Privacy Laws, Democratic regimes, Authoritarian regimes.*

I. INTRODUCTION

The rapid advancement of technology, particularly AI has led to its widespread adoption across various sectors. "The continuous research and innovation directed by tech giants are driving

[1] Author is a LLM Student at Amity Law School, Noida, India.

 [ISSN 2581-5369]

adoption of advanced technologies in industry verticals, such as automotive, healthcare, retail, finance, and manufacturing".[2] Artificial Intelligence has now become an inseparable part of our lives. From personalized recommendations in online shopping to taking financial advice, and even buying new property, AI seems to be the '*expert advise'* we rely on. A recent survey conducted by Forbes Advisor[3] reveals that consumers are interacting with AI everyday, with 43% answering that they use AI for financial planning and 30% stating that they use AI to even prepare for job interviews. While the convenience of AI has no doubt made our lives easier, it has given AI access to sensitive personal information or PII (personally identified information) which has sparked concerns surrounding the privacy and security of personal data. The handling and use of large amounts of information raises questions about respect for privacy and the rights of stakeholders. The question of how this data is collected, stored, and used became a critical concern in ongoing legislative debates about data privacy of their citizens. Consequently, legislators around the globe recognized the need for effective governance and regulations regarding data privacy to safeguard the individual privacy rights while balancing the innovation aspect of AI technology.

Different systems of governance adopted different regulatory approaches to data privacy. Democratic governments have argued both for and against such policies as policymakers seek to balance the interest of businesses, human rights, and data privacy concerns of stakeholder communities. "More authoritarian governments (and some democracies) officially cite security priorities such as counterterrorism and curtailing foreign influence as reasons to tighten control of their national digital infrastructure, ultimately enabling increased surveillance and censorship of their populations".[4] It is abundantly clear that while Democratic governments are trying to minimize the collection of data by any organization or AI systems, the Authoritarian governments wishes to gain extended control over the personal data of their citizens hence violating their Right to Privacy.

The paper seeks to analyze the regulatory approaches of Authoritarian and Democratic governments by examining key data protection frameworks in countries following a Democratic form of governance such as General Data Protection Regulation (GDPR) in Europe, the Digital

[2]*Artificial intelligence market size, share, growth report 2030*. (n.d.). Market Research Reports & Consulting | Grand View Research, Inc. https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market

[3]Haan, K. (2023, July 20). *Over 75% of consumers are concerned about misinformation from artificial intelligence*. Forbes Advisor. https://www.forbes.com/advisor/business/artificial-intelligence-consumer-sentiment/

[4]*The real national security concerns over data localization*. (n.d.). CSIS | Center for Strategic and International Studies. https://www.csis.org/analysis/real-national-security-concerns-over-data-localization

 [ISSN 2581-5369]

Personal Data Protection Act (DPDP) in India, the U.S. Data Protection Act, and other federal and state privacy laws in the United States and the countries practicing an Authoritarian regimes' such as China's Personal Information Protection Law (PIPL) and Data Security Law, Russia's Federal Law on Data Protection, and Saudi Arabia's Personal Data Protection Law (PDPL). Through this analysis, the paper seeks to highlight the contrasting approaches taken by Democratic and Authoritarian governments in governing Data Privacy. The analysis will be framed by evaluating countries falling in both the regimes on the international privacy guidelines/ standards put forth by organizations like the OECD[5] (Organisation for Economic Cooperation and Development) and UNCTAD[6] (United Nations Centre for Trade and Development), providing a comparative evaluation of how these different regimes align-or diverge-from global privacy standards.

II. THE NEED OF DATA PRIVACY REGULATIONS

Artificial Intelligence has ushered an era of unprecedented convenience which has changed the way individuals and organizations operate. Artificial Intelligence technology is trained on enormous amount of Data for it to produce accurate results and work efficiently. Artificial Intelligence is now integrated into everything from Siri and Alexa to automobiles which has granted these AI systems an access to all our information including our likes, dislikes, the people we meet, people's Name, Address, Contact number, financial details etc. The availability of this Personal Identified Information, and Collection of this data by AI systems poses the critical concern of Data Privacy. Along with that the affect of collection of data by these AI algorithms poses great threat to Economy, National Security, and Individual reputation as well.[7]

There are various ways in which AI systems are collecting and using our data such as:[8]

- Opacity and Secrecy of profiling
- Persistent surveillance
- Target Marketing

[5]*OECD guidelines on the protection of privacy and Transborder flows of personal data*. (2002, February 12). OECD. https://www.oecd.org/en/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html.

[6]*Data protection and privacy legislation worldwide*. (n.d.). UN Trade and Development (UNCTAD). https://unctad.org/page/data-protection-and-privacy-legislation-worldwide#:~:text=Data%20Protection%20and%20Privacy%20Legislation%20Worldwide%20%7C%20UNCTAD

[7] *Protecting data privacy as a baseline for responsible AI*. (n.d.). CSIS | Center for Strategic and International Studies. https://www.csis.org/analysis/protecting-data-privacy-baseline-responsible-ai

[8] Kathuria, Y., Ruhani, Vandana, Tyagi, M., & Jain, V. (2024). Protecting data privacy in the age of AI: A comparative analysis of legal approaches across different jurisdictions. *AIP Conference Proceedings, 3220*, 040007. https://doi.org/10.1063/5.0234669

- Deepfake

Opacity and Secrecy of profiling

"Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[9]. This method is used to gather, examine, and utilize information and draw conclusions based on the data about a particular group of people. This practice frequently takes place without the person's awareness or consent, which raises serious moral questions. These problems are exacerbated by AI-powered profiling because of the technology's ability to examine enormous volumes of data and find patterns that are invisible to humans. This technique and the threat of data privacy posed by it is exemplified by the Cambridge Analytica case, in which the data of millions of facebook users' was misused for political advertising[10].

Persistent Surveillance

"Persistent surveillance is a generic term that encompasses a basket of surveillance systems that share two commonalities. First, the technologies are broad and/or deep in scale and scope—for example monitoring a wide area (a city) and/or monitoring a narrow area (a home) for long periods of time. Second, the technologies allow for continuous digital collection which, when saved, allows for retrospective searches of images, people, patterns, or events."[11] The technological prowess of ongoing surveillance is demonstrated by devices like drones, facial recognition software, and AI-powered cameras. Such systems have been widely implemented in nations like China, where they are included into their social credit system, which rewards or penalizes residents according to behavior that is tracked**.** According to a study, there were 350 million cameras installed in China by the year 2020.[12] These technologies raise serious concerns about how to strike a balance between civil freedoms and public safety, even though they are frequently rationalized as being required for security.

Target Marketing

[9] *Art. 4 GDPR – Definitions*. (2018, March 29). https://gdpr-info.eu/art-4-gdpr/

[10]*Nytimes.com*. (2018, April 4). The New York Times - Breaking News, US News, World News and Videos. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[11] Ferguson, A. G. (2022). Persistent Surveillance. *The Cambridge Handbook of Surveillance Law*, 171-197. https://doi.org/10.1017/9781316481127.008

[12] Neville-Hadley, P. (2022, August 14). Inside the surveillance state: How China cows its people. *South China Morning Post*. https://www.scmp.com/magazines/post-magazine/books/article/3188545/inside-surveillance-state-how-china-coerces-its

Target marketing refers to tailoring advertisements, promotions, and product recommendations to specific audiences based on their preferences, behavior, and demographics**.** This is practiced by E-commerce platforms extensively using past data of consumers such as their purchase history, their queries and their search pattern on various other platforms. By utilizing this data, the AI technology is able to analyze when and what a consumer needs, It also helps the platforms in personalizing solid advertisement messages and showing right products. E-commerce platforms also share this data with third parties (without any prior or express consent) for marketing purposes or to improve their services. For ex: Amazon says they may share your information with third parties: as well as their own terms, users should "carefully review their privacy statements and other conditions of use".[13] Such practices can lead to potential misuse of personal information or even identity theft.

Deepfake

"A deepfake refers to a specific kind of synthetic media where a person in an image or video is swapped with another person's likeness."[14] This technique can create incredibly lifelike films, images, and audio that are frequently indistinguishable from actual content by combining deep learning algorithms with the generation of fake content. The market is overrun with deepfake software and apps, which has resulted in an increase in misleading information. A recent example of the impact of deepfake fraud is the complaint made by SP Oswal, a textile magnate and the chairman of the Vardhman Group in India, who alleged that he was defrauded by someone who set up a fake Supreme Court hearing that was chaired by someone pretending to be the Chief Justice of India, DY Chandrachud and asked him to pay Rs. 7 crore in an ongoing case against him. [15]

Such incidents are the waking call for the need of stringent data privacy regulations.

III. INTERNATIONAL GUIDELINES ON DATA PRIVACY

Since Right to Privacy is declared as human right by the United Nations Declaration of Human Rights[16] various International Organisations issues guidelines and privacy principles for organisations and legislations around the globe to help form their privacy regulations in line

[13] Calver, Miller. (2018). What tech giants really do with your data. *BBC News*. What tech giants really do with your data

[14] Deepfakes, explained. (2020, 21). *MIT Sloan*. https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

[15] LIVELAW (2024, October 1). *Scammers fake Supreme Court hearing & impersonate CJI, dupe industrialist of ₹7 crore*. https://www.livelaw.in/top-stories/scammers-fake-supreme-court-hearing-impersonate-cji-dupe-industrialist-of-7-crore-271253

[16] United Nations. (n.d.). *Universal Declaration of Human Rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

with the standards set forth. The OECD and the UNCTAD are two such international organisations that have acknowledged the need for International guidelines and principles to ensure privacy rights of individuals and free flow of data across borders.

OECD

The OECD privacy guidelines are the first International guidelines that are agreed upon by most countries. The OECD has recognized how privacy on digital space is necessary for individuals and organisations and how it can affect their interaction with the online world. There are 8 Privacy principles recognized by OECD under the **GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA.**[17] These Principles were created by the OECD to help ensure that personal data is handled responsibly.

- According to the Collection Limitation Principle, information should only be collected in a limited amount and be acquired honestly, legally, and, when necessary, with the agreement of the data subject.
- According to the Data Quality Principle, information must be accurate, comprehensive, relevant, and current for the purpose for which it is intended.
- According to the Purpose Specification Principle, the goal of data collection must be stated at the time of collection of data or prior to it, and any further usage must be limited to these goals or to modifications that are explicitly stated.
- The Use Limitation Principle states that the information should not be shared or used for purposes other than those for which it was originally intended, unless the data subject has given permission or the law permits it.
- According to the Secuirty Safeguards Principle, the necessity of acceptable safeguards against risks like loss, unauthorized access, or data misuse should be emphasized. By guaranteeing that details about data policies, procedures, and the identities of data controllers are easily accessible, the Openness Principle encourages transparency.
- According to the Individual Participation Principle, people have the right to see, examine, and, if necessary, contest or update their data.
- Lastly, the Accountability Principle ensures that data privacy is respected at every level by holding data controllers accountable for putting these principles into practice and

[17]*OECD legal instruments*. (n.d.). OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

 [ISSN 2581-5369]

upholding them.

UNCTAD

UNCTAD enacted privacy principles as a basic framework for handling *"personal data",* which is defined as information pertaining to an identified or identifiable individual who is regarded as the "data subject". The Privacy Principles were enacted to:

(i) Standardize procedures for safeguarding personal information in all UN System Organizations;

(ii) encourage ethical and open data processing that complies with each organization's requirements; and

(iii) protect people's fundamental liberties and human rights, including their right to privacy.

There were **Ten fundamental privacy principles** known as **PERSONAL DATA PROTECTION AND PRIVACY PRINCIPLES**[18] established by the United Nations Conference on Trade and Development (UNCTAD) to help UN System Organizations handle personal data in an appropriate manner.

- According to the Fair and Legitimate Processing principle guarantees that personal data is handled in a fair manner, based on permission and the best interest of the data subject. The handling of such should be in accordance with the mandates of UN and other legal requirements.
- According to the Purpose Specification principle, the purpose of collecting the data should be well-defined and it should uphold people's liberties and rights without straying into incompatible uses.
- According to the principle of proportionality and necessity, data processing should be used in that proportion only which is necessary to fulfill the stated purpose
- According to the Retention Principle, the data should be stored or retained for as long as it fulfills the purpose.
- According to the Accuracy principle, the data so obtained should be accurate and updated so that intended purpose could be fulfilled.
- According to the Principle of Security, appropriate safeguards measures should be taken

[18]*Principles on personal data protection and privacy | United Nations*. (n.d.). United Nations - CEB. https://unsceb.org/principles-personal-data-protection-and-privacy-listing

by organisations in order to secure the personal data.

- According to the principle of confidentiality, organisations are required to maintain the confidentiality of the data.
- According to the transparency principle, data processing operations must be transparent, telling people about data use, access rights, verification, and, if practical, rectification choices
- According to the principle of Transfer, Data transfers to third parties should only take place where sufficient data protection is guaranteed.
- According to the Accountability principle, a commitment to responsible data practices by the UN System Organizations is established. It required UN organisations to have efficient policies and procedures to guarantee adherence to these privacy principles.

Both of these organisations has laid down a comprehensive roadmap for privacy regulations across the globe. The recognized principles by both the organisations are largely similar that requires Data Principle or Data subject to be informed about the collection and purpose of collection of data. It also requires the collecting entity to maintain confidentiality of data, privacy of data by not sharing it with any third party, and use the data for the purpose specified.

IV. COMPARATIVE ANALYSIS OF DATA PRIVACY REGULATIONS IN AUTHORITARIAN VS. DEMOCRATIC REGIME

Data privacy is the subject of legislative debates around the globe since the extended proliferation of AI in day to day lives. AI has led to significant collection, processing, and utilization of data. The process of how this data is collected is unknown and leads to various ramifications such as infringement to privacy rights of individuals, and organisations alike. This also leads to data breaches and other types of cyber crimes. To combat with data theft on the digital space, proper data privacy regulations are required. Different governance regimes have taken a different approach to regulate data privacy in their countries.

(A) Authoritarian regime

1. China

Personal Information Protection Law, 2021[19]: This regulation is based upon on the principles of Collection Limitation, Accountability, and Purpose Specification Principle. PIPL of 'Natural persons' of China both domestically and abroad. PIPL requires explicit consent from users for

[19] *The PRC personal information protection law (Final): A full translation*. (2021, December 29). https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation

data collection and processing.

- The most important provision of the act is that as per Article 13, the act allows only CONSENT based collection, sharing or storing of data
- The Article 5 of the act recognizes various principles to collect, store and process personal information of *natural persons* of china that is Legality, Legitimacy, necessity and good faith.
- Article 7 of the act mandates the organization to be *transparent* about their collection methods, the purpose of collection of the information.
- Article 9 of the act ensures that necessary measures should be taken by the organisations to protect the information so collected.
- Through section 11 and 12 the government takes appropriate measures to protect the flow of personal information and punish the infringement of personal information along with regulating the cross-border flow of information.
- PIPL also imposes fines for non-compliance up to RMB 50 million ($7.8 million) for enterprises with an annual revenue exceeding RMB 50 million ($7.8 million).

2. Russia

Russia passed the law on privacy of Personal data in the beginning of 20th century. The Federal Law-149 fz on Information, Informational technologies, and protection of Information[20] passed in the year 2006. This law whereas provides the holder of information the right to protect and share the information, it also gives the Russian Federation a greater right to demand the access of any information. The law also makes the information shared with the state's institutes such as museums & Libraries public. This law is based on free flow and dissemination of information for proper education and knowledge of citizens. The law places great reliance on protection as well as dissemination of required information by Russian Federation, and state and local governments.

- The Article 6 of the act provides that the "holder of information" shall decide who may access his information, when to share the information, or how the information may be used except otherwise stated by the Federation. The act places a greater reliance on the *holder* to take necessary precautions for protection of such information.

[20] Federation council, Russia. (2006). *FEDERAL LAW NO. 149-FZ OF JULY 27, 2006 ON INFORMATION, INFORMATIONAL TECHNOLOGIES AND THE PROTECTION OF INFORMATION*. World Trade Organization - Global trade.

- Article 8 (4) of the act provides that,
- **"**No restrictions may be imposed on access to:
- 1) statutory legal acts affecting the rights, freedoms and obligations of person and citizen and also those establishing legal status of organisations and the powers of state power bodies and local selfgovernment bodies;
- 2) information on the state of the environment;
- 3) information on the activity of state power bodies and local self-government bodies and also on the use of budgetary funds (except for data constituting state or official secrets);
- 4) information accumulated in the open funds of libraries, museums and archives and also in state, municipal and other informational systems set up or intended to provide citizens (individuals) and organisations with such information;
- 5) other information the impermissibility of restriction on the access to which is established by federal laws."[21]

3. Saudi Arabia

After much anticipation, Saudi Arabia enacted its Personal Data Protection Law[22] in the year 2021. This Law sets stricter standards for Data privacy following the global principles. The PDPL act is based on 7 Privacy Principles which are Accountability, Lawfulness, fairness, and Transparency, Purpose Limitation, Data Minimisation, Accuracy, Storage Limitation, and Integrity & Confidentiality.

- Article 4 of the act provides that there should be a legal basis for the collection of the data. Data subject shall have the Right to know how his data is being collected, what is the purpose of collection of this data, correction and updating of his data, and the right to destruct the data as well.
- Article 10 of the act prohibits the controller from obtaining Data subject's information from a third party.

However, Article 6 and Article 10 of the act also provides extended rights to controller to process the data without express consent of the data subject. Certainly there are conditions attached to it, but it shall give the controller the opportunity to exploit such provisions and use

[21] *Supra note 20*

[22]Saudi Data & AI Authority. (2023). *Personal Data Protection Law*. https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20Data%20English%20V2-23April2023-%20Reviewed-.pdf.

the provisions for their benefits.

(B) **Democratic Regime**

4. EUROPEAN UNION (EU)

General Data Protection Regulation (GDPR) of 2018[23]

European Union in purview of increasing risks to data privacy enacted the General Data Protection Act in 2018. As per the European Union, *"The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world"* [24]. The GDPR applies to all the organisations that process personal Data of citizens of European Union. It is also to be noted that GDPR extends to all the companies outside EU as well if they are in any way tracks or utilises the data of citizens of EU.

- Article 5.1.2 of the act provides seven protection and accountability principles that should be followed in order to process the data of EU citizens which are consistent with the privacy principles provided by OECD & UNSTG
- GDPR mandates obtaining explicit consent from users for data collection and processing under Chapter 3, Article 13,14,15, whereas Article 17-20 of chapter 3 section 3, grants users the right to access, rectify, erase, restrict, and object to their data's processing.
- Article 25(1) of the act mandates Data controller to take appropriate measures to protect users' data and use techniques such as pseudonymisation and Data minimization.
- The act also establishes competent authority to deal with possible data breach such as article 33 of the act provides for taking action under 72 hours in case of a possible data breach by a data controller
- The act imposes significant fines for non-compliance, up to €20 million or 4% of global annual revenue (whichever is greater).

5. United States Of America

The Algorithmic Accountability Act of 2023

"The Algorithmic Accountability Act of 2023 requires companies to assess the impacts of the AI systems they use and sell, creates new transparency about when and how such systems are used, and empowers consumers to make informed choices when they interact with AI

[23] (2022, September 27). General Data Protection Regulation (GDPR). https://gdpr-info.eu
[24] *What is GDPR, the EU's new data protection law?* (2023, September 14). GDPR.eu. https://gdpr.eu/what-is-gdpr/

systems"[25]. "The Algorithmic Accountability Act" of the US stands out for its extensive framework in addressing algorithmic decision-making transparency. It mandates companies to assess and mitigate biases and privacy risks inherent in their algorithms, promoting accountability in AI-based profiling[26].

- The Act addresses this issue by the virtue of Section 4(a)(4)(E)[27] which says that *" an evaluation of any differential performance associated with consumer's race, color, sex, gender, age, disability, religion, family status, socioeconomic status, or veteran status, and any other characteristics the Commission deems appropriate (including any combination of such characteristics) for which the covered entity has information, including a description of the methodology for such evaluation and information about and documentation of the methods used to identify such characteristics in the data (such as through the use of proxy data, including ZIP Codes)."*

6. India

Data Protection Laws: DPPD Act of 2023[28]

The Data Protection Act (DPA), was enacted in the year 2023. This act aims to regulate the processing of personal data available digitally i.e. on the internet space, by organizations operating within or outside India that process data related to individuals residing in India. The focus of the act is primarily on the protection of personal data and the rights and duties of data principals.

- Section 2 (u) of the act defines 'Personal data breach' and includes any any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data online.
- Section 2(x) of the act talks about 'processing' of personal data that includes processing, storing, collection, transmitting or permitting/preventing of personal data.
- Section 4 of the act has provided for various grounds of using personal data, by data fiduciaries and has disabled third-party sharing of data. The provision of the act

[25] Wyden, R. (2023). *Algorithmic Accountability Act of 2023 Summary*. https://www.wyden.senate.gov/imo/media/doc/algorithmic_accountability_act_of_2023_summary.pdf.)

[26] *H.R. 5628 (IH) - Algorithmic Accountability Act of 2023*. (2022). https://www.govinfo.gov/app/details/BILLS-118hr5628ih

[27] id

[28] Ministry of Electronics and Information Technology, Government of India. (2023). *Digital Personal Data Protection Act 2023*. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

expressly 'A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose'.

V. CONCLUSION

Artificial Intelligence as a technology has potentially being integrated into all the aspects of our lives. This technology has made the lives of human easier, with giving answers in seconds, to help people and organisations with pretty much anything. To answer efficiently, this AI based technology is trained on enormous amount of data that is scratched off internet without the express consent of the data principal or the data subject. The utilization and collection of this data infringe the right to privacy of people. To protect the right to privacy of people, countries around the globe are required to come up with data privacy regulations. However, it is pertinent that the countries with different governance regimes shall have different approaches to data privacy. To provide a comprehensive approach for data privacy, there are Global standards of privacy being setup by OECD, and UNCTAD. These organizations provide certain principles for data privacy that may be followed while drafting and enacting data privacy regulations by countries. The countries with authoritarian regime have partially followed the principles setup by these organizations. These countries have provided the *data subjects* the right to restrict or provide access for their data, and the right to be informed about the processing, purpose of collection and the time period for utilization of the data. However, these countries have also granted the central governments or the state government a higher right to retain data, or to access information without the consent of the data subject. Whereas, countries that follows the democratic regime have followed these global principles of data privacy and enacted their regulations in line with these international mandates. These countries have provided the absolute right to *Data principals* over their data. Certainly, these have also included the access to the data in case of National emergency or in matters of national security. In conclusion, the international mandates have been followed by all the six countries in accordance with their governance regime.

*****

 [ISSN 2581-5369]