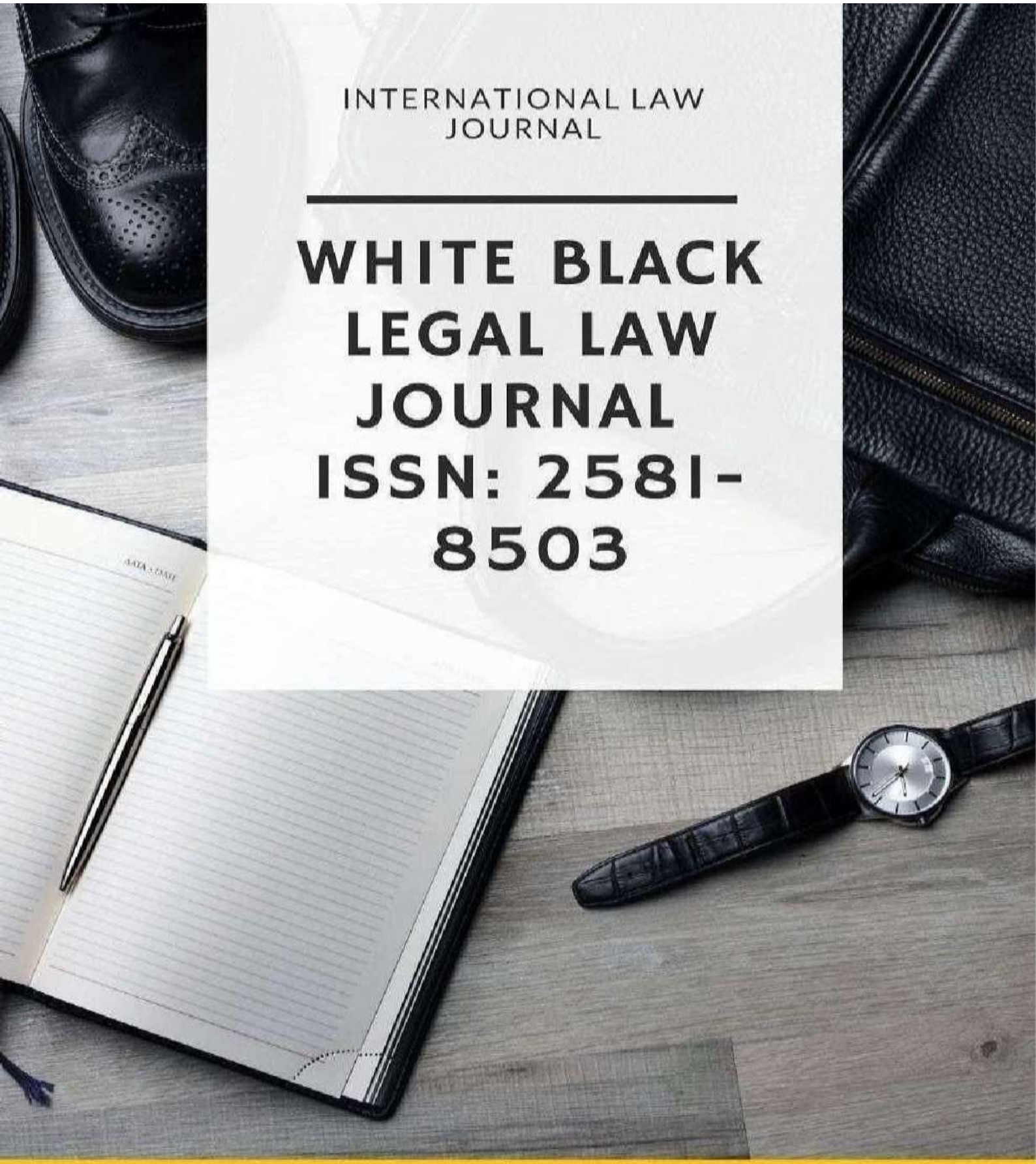

INTERNATIONAL LAW JOURNAL

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.

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi, Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur,
M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

AI HAMPERS PRIVACY AND ANALYSIS OF DIGITAL PERSONAL DATA PROTECTION ACT 2023

AUTHORED BY - DHATCHAYINI AMARNATH
& MINNILA PRIYADARSHINI S

1. INTRODUCTION:

Artificial intelligence is flourishing extensively, unleashing waves of technical and social change. It is increasingly preferred in various fields due to its ability to simplify complex tasks. Generative AI, capable of creating texts and images, plays a vital role in influencing societal decisions. Unfortunately, bad actors exploit AI to spread misinformation, such as using AI-generated images, like one depicting the Pentagon burning, which can spook equity markets. Therefore, responsible AI practices are crucial, considering the impact on individual privacy and security.

Although the government introduced the Digital Data Protection Act in 2023, guaranteeing absolute security remains challenging. Prior to this act, there was no legislation addressing data protection. The current bill, with provisions for a Data Protection Board and Data Fiduciary, aims to efficiently safeguard privacy. However, despite these efforts, risks persist. This paper explores the ongoing challenges and risks to privacy post the enactment of this act in India, focusing on the significant challenge posed by the integration of AI into governance.

There is an assumption that AI will soon be utilized for decision-making, potentially replacing judges in the court system. Nevertheless, programming a computer to be inherently ethical is challenging. Machines lack the capacity for ethical considerations; they operate solely based on algorithms. As the government may eventually delegate decision-making to machines, questions arise regarding accountability. Who will be held responsible Whether the developer of AI or official who relied on AI and AI systems cant be punished as they cannot bear guilt ,its difficult to inbuild ethics into ,machines and justice cant be delivered to parties .AI affects privacy and has bad effects on society furthermore generates unethical decisions ,it can be resolved through Identity assurance framework

and information integrity .

1.1 AI HAMPERS PRIVACY:

AI research is expanding at a rapid pace in today's world, with an annual growth rate of 12.9 percent over the last five years. India stands as the third-largest country in AI research output, following China and the USA. AI systems, crucial for their functioning, often rely on substantial amounts of personal data for learning and making predictions. This reliance raises concerns about the collection, processing, and storage of such data. As Artificial Intelligence continues to evolve, the involvement of personal information intensifies, making the proliferation of data breaches a major problem in the current digital scenario.

Generative AI, a powerful tool, can be misused to create fake profiles or manipulate images. Similar to other AI technologies, it heavily depends on data. Cybercrimes impact the security of 80% of businesses worldwide, emphasizing the significant consequences of personal data falling into the wrong hands. Active measures must be taken to safeguard customer information by employing authentication through data platforms.

AI systems inherently carry the potential for bias and discrimination due to their reliance on personal data, often leading to harmful outcomes for individuals. Another major concern is the use of AI in job recruitment, where strict procedures may result in job displacement without the awareness of the applicants. The algorithms employed by AI are deemed dangerous because the collection of personal data lacks transparency, making it uncertain how data is gathered.

The primary privacy concern associated with AI revolves around the collection and processing of personal data for various purposes, posing a high risk of data breaches and unauthorized access. There is a potential for such information to fall into the wrong hands through hacking or other security issues, with bad actors using the information for malicious purposes. This creates a severe impact on people's lives, such as the creation of fake accounts using personal details or the inappropriate use of AI to manipulate images.

Given AI's increasing reliance on personal data, the Digital Personal Data Protection Act of 2023

needs thorough analysis to assess how effectively it protects personal data from AI without compromising privacy, as its aim is to process personal data for lawful purposes.

The adoption of the DPDP bill in Parliament comes six years after the landmark case of Justice K.S. Puttuswamy v Union of India. In this case, the Supreme Court of India recognized a fundamental right to privacy, including informational privacy, within the "right to life" provision of India's Constitution. The bill seeks to provide protection for personal data collected within and outside the territory of India to secure the privacy of individuals.

1.2 REVIEW OF LITERATURE:

It is asserted that personal data of individuals is being extensively misused, primarily due to the presence of biometric identity systems, surveillance, and the Aadhar system in India. The information provided for Aadhar cards is being exploited in numerous instances, and India faces significant challenges in dealing with with protection policy and Europe has strong data protection regulations when compared to India .[1]

Research Gap: It's not solely due to individuals providing personal data for these systems; there are various other contributing factors, such as web portals, social media, and the use of AI tools, that are responsible for exploiting personal data. Personal data is available on various digital platforms without the knowledge of the individuals involved.

It is asserted that data protection authorities address the importance of ensuring privacy protection in AI. Privacy is impacted due to advanced algorithms. AI guarantees the limitation and deletion of personal data after its original purpose, providing assurance. However, efforts to reduce risk weaken data protection and diminish the benefits obtained from AI.

It is challenging for AI to maintain transparency. The statement suggests that AI can facilitate ethical decisions and ensure lawfulness, transparency, and fairness. AI uses the personal data of Individual

[1] Pam Dixon,A failure to do no Harm India's Aadhaar biometric ID program and its inability to protect privacy ,7,539-567(2017)

for said purpose and there are less chance for exploitation .[2]

Research Gap: Privacy is not solely impacted by the algorithms used by AI; rather, it is predominantly influenced by bad actors who exploit personal data for unlawful purposes, thus violating individuals' privacy. AI tends to use personal data beyond the stated purpose outlined by the data principal, making assurance challenging. However, it is possible to mitigate privacy risks without compromising the benefits of AI.

AI is limited in its ability to produce ethical decisions as it operates solely based on algorithms. Acting mechanically, it lacks awareness of moral and ethical principles and does not exhibit a human-centric approach, posing potential problems in the future.

First and foremost, a responsible data governance strategy must integrate robust programs in both information security and privacy. Any collected and retained data carry inherent breach risks. The most effective approach is to limit data collection to the essentials and refrain from retaining data that is no longer business-critical. Retained data, such as lists of active customers and their billing information, should be secure from external hackers and insider misuse.

Furthermore, retained data should be associated with metadata that indicates provenance, sensitivity, and any legal or contractual limitations on use. For instance, commercially procured data may have usage restrictions specified in contracts with vendors. Legal considerations, such as the Fair Credit Reporting Act in the United States, may prohibit the use of certain factors in credit or employment decisions, even when the collection of such sensitive information is legally permissible.

Data should undergo encryption both at rest and in transit. Encryption keys should be subject to appropriate access control mechanisms, ensuring that sensitive customer data is accessible only when and where necessary, and solely by employees with verified access needs. Continuous monitoring of sensitive data stores is essential to enable the auditing of queries against them. This enables later correlation with approved business needs. As the litany of major recent data breaches and privacy

[2] Christopher Kunar - “Expanding the Artificial Intelligence Data Protection Debate 2018, vol 8, no :4)

failures shows, a firm information security posture and a robust privacy program are the foundation for any responsible data governance strategy.[3]

Research Gap:

Encrypting data does not guarantee privacy at all times, as bad actors constantly devise new techniques to manipulate personal data. AI, in its current state, may struggle to ensure that personal data is used exclusively for its intended purpose. Numerous incidents are emerging where personal data is used without the consent of the individuals involved.

In comparison to the GDPR from the EU, the Digital Personal Data Protection Act (PDPB) is narrow. The GDPR's regulations on privacy provide extensive protection, particularly regarding the transfer of personal data. Privacy laws in Europe are stringent, requiring notification to individuals if their personal data is utilized. GDPR also stipulates that an individual's data is not subject to automatic decision-making. In contrast, the PDPB does not grant the same right, highlighting its potential limitations in effectively safeguarding individual privacy strictly .[4]

1.3. PROBLEMS IN DPDP ACT 2023:

PRIVACY ISSUES:

The Digital Personal Data Protection Act, 2023 (DPDP Act), is now a looming reality, marking India's introduction of a new data privacy legislation. This law sets compliance expectations for data fiduciaries (entities collecting and processing digital data) concerning their data principals (individuals to whom the data belongs). The enactment of this law has provided a sense of relief, especially at a time when the use of artificial intelligence-based applications, trained on substantial amounts of personal data, is gaining popularity. Despite the assurance that personal data must be collected and processed in accordance with the law, several gaps and unanswered questions arise from India's Digital Personal Data Protection Act, 2023

[3] . A. Kroll, "Data Science Data Governance [AI Ethics]," in IEEE Security & Privacy, vol. 16, no. 6, pp.
[4] Pratiksha Ashok ,The curious case of automated decision making in India ,Vol 4 235-248

LEGITIMATE PURPOSE:

There is no provision in the Digital Personal Data Protection Act, 2023 (DPDP Act) that specifically regulates the purpose for which data can be collected and how it can be used, as long as the purpose is deemed legitimate. As currently enacted, the law allows data fiduciaries to collect data for any legitimate purpose, provided it is legally permissible. This implies that algorithms tracking personal preferences and pushing targeted advertisements exploiting personal data and online behavior (commonly known as dark patterns) will continue without mitigation, except in the case of children. Given that India's Digital Markets Act has not yet been drafted, and there is no regulation on the use of AI-based applications, data use for legal but unethical purposes may still thrive in India. Moreover, in the case of children, while the law mandates obtaining the consent of the parent/guardian, the process for legitimately verifying such consent remains entirely unclear.

PUBLICLY AVAILABLE DATA:

Clause 3(c)(ii) of the Bill states that the Act shall not apply to personal data that is made or caused to be made publicly available by the user to whom such personal data relates. For example, if you are a blogger and have made your personal data publicly available through social media while blogging, then the processing of that data won't fall under the purview of the data protection law.

This clause significantly impacts how AI companies can access and process people's publicly available data in India for AI development purposes**.**

DATA PROCESSED BY BAD ACTORS:

Privacy is not solely affected due to algorithms present in AI but also because of the presence of many bad actors using unlawful means to violate the privacy of individuals. Cybersecurity issues are on the rise as bad actors utilize AI to spread fake information in society, influencing the decisions of many people.

This paper aims to address several of these ambiguities as the provisions of the DPDP Act are litigated before the judiciary.

1.4. RESEARCH METHODOLOGY:

Basically, it's a Doctrinal research methodology that focuses on analyzing and interpreting various secondary data's such as Legal statute, Articles, Journals, Case laws, newspapers and Books. We specifically analyze about Digital personal Data protection act 2023 in brief and to collect more from Articles.

1.5. RESEARCH QUESTIONS:

1.) Whether the Digital Data Protection Act be effective in safeguarding privacy from malicious actors?
2.) Whether this act potentially cause confusion, considering its basis on the General Data Protection Regulations from the European Union?
3.) Whether the Data protection act gives more authority to the government in processing the personal data?
4.) Whether AI can produce ethical decisions?
5.) Whether there's any regulation to mitigate the algorithms that keep track of your personal preferences, and push advertisements that take advantage of your personal data and online behavior (dark patterns)?
6.) Whether the exception under Clause 3(c)(ii) of the Bill (the Act shall not apply to personal data that is made or caused to be made publicly available by the user to whom such personal data relates) hampers privacy or not?

1.6. SCOPE AND LIMITATION OF STUDY:

Scope of research is limited to Digital data protection act, Privacy and ethical considerations of AI. We focus more about the efficiency and effectiveness of the act in protecting personal data of Individual, Use of AI by bad actors is great threat they influence the people in a bad way .

2. ATTRIBUTES OF DPDP ACT 2023:

This act was enacted in 2023 following the drafting of multiple bills by the parliament in 2018 and 2019. The realization that the right to privacy falls under the ambit of the right to life prompted the

government to introduce a statute for the protection of individuals' personal data. The main objective of the act is to process digital personal data of people for lawful purposes, and it is enacted based on the General Data Protection Regulation. from European Union .[5]

The act has introduced various key roles, including Data Fiduciary, Data Principal, Data Protection Board, Significant Data Fiduciary, Data Processor, Data Protection Officers, and Consent Manager. These roles are essential in determining the necessity for processing personal data and ensuring it is processed only for lawful purposes.

The act is organized into the following chapters:

i) Obligations of Data Fiduciary
ii) Rights and duties of Data Principal
iii) Data Protection Boards

DATA FIDUCIARIES:

The act takes a cautious approach to processing personal data and explicitly states that data will be processed only for legitimate purposes and with the consent of the Data Principal. Data Fiduciaries play a crucial role as they determine the purpose and means for processing personal data. They are obligated to use the personal data only for the stated purpose and to the extent of the consent given by the Data Principal, not beyond that. The consent given by the data principal should be free, specific and informed for specified purpose.[6]

DATA PROCESSOR:

They process personal data under the guidance of the data fiduciary and are recognized by the DPDP Act, bound to fulfill obligations in a proper manner while complying with the law. If data is processed, it cannot be retained; it must be deleted if a data principal withdraws consent, and proper information on how personal data is being processed must be provided to the subject.

[5] Anirudh Bhurman, Carnegie India, oct3,2023 https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624
[6] Ministry of electronics & IT, PIB Delhi ,Aug 9 ,2023 ,pib.gov.in

UNIVERSAL APPLICABILITY OF DPDP ACT:

The act processes personal data available within and outside the territory of India, collected in both digital and non-digital forms through various mediums. It does not restrict the transfer of personal data outside India, aligning with GDPR principles and having a similar effect. The act aims to protect the privacy of data beyond the Indian territory, exhibiting a broader impact.

PRINCIPLE OF CONSENT:

Consent from the data principal is crucial for processing personal data for lawful purposes. It involves two factors: voluntary permission to access and legitimate use. Consent cannot be obtained through fraud or coercion. Prior notice must be given to the subjects, clearly stating the legal purpose and specifying the manner in which personal data will be processed be intimidated to data principal and can later withdraw their consent through consent manager and should delete after the said purpose .

Section 3:

Clause 3(c)(ii) of the Bill specifies that the Act does not apply to personal data made or caused to be made publicly available by the user. For instance, if a blogger publicly shares personal data through social media while blogging, the processing of that data falls outside the scope of data protection law. This clause significantly impacts how AI companies can access and process people's publicly available data in India for AI development purposes.

DATA PRINCIPAL:

Data principals, being citizens, enjoy multiple rights ensuring the protection of their personal data without exploitation. These rights include the right to privacy, the right to access information about how their personal data is processed, and the right to correction of misleading data. Importantly, data principals have the right to grievance redressal and can approach the data protection board to resolve disputes. They also have the right to nominate another person in case of death.

DATA PROTECTION BOARD:

The Data Protection Board has the power to take cognizance of cases only after a complaint is received from a data principal regarding the intimation of personal data breach or on a reference made by the central government. While it can enquire into cases and levy penalties, the board cannot take

cases on a suo moto basis, indicating a lack of discretion to protect individual privacy. It is not an independent body and should be given more powers to effectively safeguard citizen privacy.

SIGNIFICANT DATA FIDUCIARY:

Significant data fiduciaries, notified by the central government under section 10, are appointed for special purposes to safeguard the security of the state. They are obligated to appoint a data protection officer to resolve disputes with data principals.

Exemptions From Obligations of the Act:

The Act provides exemptions, allowing personal data to be used for enforcing legal rights or claims, court or tribunal proceedings, financial information purposes, and to protect the sovereignty and integrity of India. However, these exemptions grant significant autonomy to the government in processing personal data, potentially undermining privacy protection under the law.

PENALTY:

Monetary penalties are imposed, with no imprisonment, based on the nature and gravity of the offence. The fine amount varies case by case, depending on the situation.

3. SHORTCOMINGS OF DPDP ACT 2023 DUE TO THE PRESENCE OF AI:

The original objective of the act was to process digital personal data for lawful purposes, but the presence of AI introduces a lack of clarity on how the act will control data processed by these systems, leading to a deficiency in relevant provisions.

We cannot entirely trust data fiduciaries as they might struggle to identify the lawful purpose to process personal data, leaving room for potential unethical use and manipulation by bad actors. The act fails to precisely define what constitutes a legitimate purpose, creating ambiguity that could impact individual privacy. The definition of consent is also lacking, posing potential challenges in the future. There is a significant risk of AI processing personal data in the name of legitimate purposes and misusing it, as AI relies on collecting data through various modes, raising concerns about privacy and

posing a substantial threat.

The act does not extend protection to publicly available personal data, showing bias and inadequacy in safeguarding individual privacy. This leaves personal data exposed to potential exploitation and misuse by AI companies, particularly from various public platforms like social media, biometric details, and Aadhar systems. The Digital Personal Data Protection Act does not seem to prioritize privacy and security adequately.

AI introduces complications as personal data may be retained beyond the specified purpose, and the act lacks provisions to control AI's data collection methods. Data fiduciaries cannot effectively monitor or control AI to stop processing personal data once the stated purpose is achieved, creating uncertainties and a lack of assurance.

When AI processes personal data, data principals may be aware, but the inability of the data protection board to take suo moto actions against AI presents challenges. There is no clear provision on how to hold AI accountable for personal data breaches, causing confusion about whether developers or officials who rely on AI should be made liable. This has resulted in unnoticed scams and cybersecurity issues, leading to breaches of individual privacy.

The act appears more focused on protecting the sovereignty and interests of the state than on securing individual privacy. The exemption section grants the government significant autonomy to process personal data to maintain public order, with minimal concern for individual privacy. It should be more individual-centric.

The penalties outlined in the act are not stringent, providing only for monetary penalties without imprisonment. This leniency could embolden bad actors to exploit privacy with minimal fear of consequences. AI algorithms used by bad actors to spread fake information pose a severe threat to individual privacy, and the act's silence on this issue leaves the data protection board unaware of how to address privacy issues caused by AI.

The act permits data fiduciaries to collect data for any legitimate purpose, as long as it is legally

permissible. This opens the door for algorithms to track personal preferences and push advertisements based on personal data and online behavior, known as dark patterns. The act needs swift implementation for effective regulation of digital markets, especially considering the absence of the Digital Markets Act in India.

4. REMEDIES TO SECURE PRIVACY:

Blockchain technology can be integrated to secure and execute transactions in an open network without involving any third party. By combining blockchain with AI, the algorithms and digital signatures used by AI can be made more privacy-friendly and enhance security.

Data anonymization should be mandated on all websites by domain owners. This ensures that data collected cannot be directly associated with individuals, instilling trust in websites and safeguarding individuals' privacy.

The DPDP Act of 2023 requires necessary amendments to make it more individual-centric. It should prioritize protecting the privacy of individuals over granting extensive power to the government in accessing personal data under the guise of state security. Publicly available data should also be afforded protection.

The Data Protection Board must be endowed with regulatory powers to frame rules and a code of conduct. This will enable it to work efficiently in protecting individual privacy and create provisions to address data breaches caused by AI. Legitimate purposes must be properly defined.

An identity assurance framework should be established by all online websites. This framework's ability to determine the true identity of the claimant with a certain level of certainty is crucial for trust. Such frameworks should be mandatory for all domain owners.

Information integrity should be made mandatory in all cyberspace. It ensures the trustworthiness of information stored in a cloud database, free from corruption, and ensures that customers can rely on information with confidence, guaranteeing privacy.

5. CONCLUSION:

Undoubtedly, AI has the potential to revolutionize our lives, but it also brings serious concerns about privacy. As AI becomes more prevalent, the collection and analysis of vast amounts of personal data pose both positive and negative implications. Even after the DPDP Act of 2023, there are ongoing reports of personal data being hacked and exploited, indicating the need for further improvements and amendments to enhance individual privacy, especially in the context of AI.

The Data Protection Bill should be more individual-centric, prioritizing privacy over granting sovereign immunity to the government for processing personal data. The pending India's Digital Markets Act needs prompt drafting and implementation. It is crucial to ensure responsible development and deployment of AI by transparently and ethically collecting and using personal data. Clear guidelines on data usage and sharing, along with safeguards to prevent misuse, are essential. Mechanisms for individuals to control their data should be developed.

Ultimately, promoting responsible AI development requires collaboration among policymakers, industry leaders, and civil society. Policies and practices supporting the responsible use of AI technologies should be incorporated into the DPDP Act of 2023.

BIBLIOGRAPHY:

Secondary sources

JOURNAL ARTICLES

- Pam Dixon,A “failure to do no Harm India’s Aadhaar biometric ID program and its inability to protect privacy” ,7,539-567(2017)
- A. Kroll, "Data Science Data Governance [AI Ethics]," in IEEE Security & Privacy, vol. 16, no. 6, pp.
- [1] Pratiksha Ashok ,The curious case of automated decision making in India ,Vol 4 235-248
- Christopher Kunar - “Expanding the Artificial Intelligence Data Protection Debate 2018, vol 8, no :4)

NEWSPAPER

Aditya Sinha, Can AI be ethical and Moral, THE HINDU ,August 24,2023,9

INTERNET

- Anirudh Bhurman, Carnegie India, oct3, 2023 https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624
- Ministry of electronics & IT, PIB Delhi, Aug 9, 2023, pib.gov.in
- Dr. Mark Van rijmenam, The digital speaker, Feb 17,2023 https://www.thedigitalspeaker.com/privacy-age-a