INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions ofthe authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsever for any consequences for any action taken by anyone on the basis of information in theJournal.

Copyright © International Journal for Legal Research & Analysis

 ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur.Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time &Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

FORENSICS AND AI: ANALYSING DEEPFAKE, DATA MANIPULATION, AND ENCRYPTION

AUTHORED BY - JYOTHIKALAKSHMY PRABHA,
LLM student, School of legal studies, Cochin University of Science and Technology,

ABSTRACT

The intersection of forensics and artificial intelligence (AI) presents significant challenges, particularly in the domains of deepfakes, data manipulation, and encryption. This paper examines the latest legislative frameworks designed to address these concerns, focusing on the EU's Artificial Intelligence Act and India's Draft Digital Personal Data Protection Rules, 2025. The analysis begins with an overview of deepfake technology, exploring its forensic implications and the risks it poses to information integrity. It then examines data manipulation techniques, their legal ramifications, and the necessity for proactive regulatory responses. Additionally, encryption technologies are analyzed within the framework of evolving data protection and cybersecurity legislation, highlighting their role in forensic investigations. As AI-driven manipulation tools continue to advance, ensuring both security and accountability becomes paramount. This study provides a critical assessment of current legislative measures and proposes enhancements to address the unique challenges posed by AI in digital forensics. By advocating for regulatory clarity and balanced oversight, the paper aims to safeguard individual rights while fostering responsible AI innovation.

Key words: forensics, deepfake, AI, Data manipulation, legislation

INTRODUCTION

The intersection of forensic science and artificial intelligence (AI) is changing digital investigations in a way whereby there's a new facility to process and analyse enormous digital data with great speed and efficiency.[1] Nonetheless, this intersection of ICT and law introduces colossal challenges, not least in regard to the rise of such advanced techniques as deepfakes and data manipulation and the complications arising from encryption.[2] These technologies can

[1] Use of Artificial Intelligence in Digital Forensics, EM360TECH <https://em360tech.com/tech-articles/use-artificial-intelligence-digital-forensics> accessed 1 February 2025
[2] Digital Forensics and Artificial Intelligence, Simply Forensic <https://simplyforensic.com/digital-forensics-and-artificial-intelligence/> accessed 5 February 2025

 ISSN: 2582-6433

be beneficial but can also potentially be exploited and threaten the justice system in serious ways: they can be used to destroy evidence integrity, manipulate information, and cloud illicit activities.[3] As AI-driven tools grow in useful capabilities, digital forensic scientists, in order to maintain their accountability and security, are warranted to take significant steps to avoid similar crime provocations.

Complexity and sophistication of cyber threats increasingly demand a proactive and adaptive approach to digital forensics. Cybercrime evolves at such a pace that conventional forensic techniques can barely keep up. Therefore, future options for using artificial intelligence (AI) technology to strengthen investigative capabilities such as digital evidence automated analysis, identifying suspicious patterns, and providing underlying communications in unstructured data. AI forensics, however, raises some concerns, including the reliability and accuracy of AI tools, algorithmic bias potential, and interpretation issues around use of AI model.[4]

This research paper discusses the various issues and prospects that AI along with digital forensics bring with it, focusing particularly on the deepfake data manipulation and encryption. In particular, it gives an overview of deepfake technology and its forensic implications as well as addresses different techniques of manipulating data with their legal implications, and scrutinizes the role of encryption in protecting data but complicating forensic analysis. Further, this research reviews the present legislative frameworks-the EU's Artificial Intelligence Act and India's Draft Digital Personal Data Protection Rules, 2025-in dealing with the issues. Through advocating regulatory clarity and balanced oversight, this paper seeks to suggest improvements to existing laws, protect individual rights, and allow responsible AI development in digital forensics.

FORENSICS AND AI

AI is not only transforming its practice into modernized forensic investigations but also revolutionizing the whole forensic science field by improving precision, efficiency, and investigative capacities. It is indeed reshaping the daily practice of forensic professionals, heralding a new era in solving crimes. With the capability to recognize much more complex

[3] CBDT Releases Digital Evidence Investigation Manual, Taxguru (n.d.) <https://taxguru.in/income-tax/cbdt-releases-digital-evidence-investigation-manual.html> accessed 5 February 2025

[4] Unveiling the Impact of Artificial Intelligence in Forensic Science, Geeta University Blog (n.d.) <https://blog.geetauniversity.edu.in/unveiling-the-impact-of-artificial-intelligence-in-forensic-science/> accessed 5 February 2025

 ISSN: 2582-6433

patterns in data, such as fingerprints and DNA, faster and much more effectively than humans, AI can vastly improve the interpretation of forensic evidence. In addition, analysis with AI systems remains untied from human factors, such as fatigue and bias, whereas the performance of automated routine tasks cuts down on the likelihood of human error. Besides, its ability to process large amounts of data reveals previously unnoticed correlations, and AI assists investigators in constructing a more exhaustive case via cross-referencing varied types of evidence.[5]

But there are challenges that need to be considered: ethical issues, the possibility of algorithms containing bias, and the much needed transparency and reproducibility in AI processes. Lack of general knowledge on AI in law enforcement and legal personnel is also a barrier to the effective use of AI. AI models are created and maintained using massive amounts of data, and an absence of standards on what constitutes valid data can lead to wrong conclusions being made.[6]

It is possible that the applications of artificial intelligence in forensic science extend to crime scene analysis and facial recognition, DNA analysis, and cyber forensics. AI-powered drones will scan the crime scene, while facial recognition will speed up the suspect identification process, and AI will enhance biometric technologies. In digital forensics, AI automates and speeds up the evidence collection and analysis process from digital devices. Collaboration among researchers, law enforcement, and AI developers is key to shaping the future of AI in forensic science. Integrating AI and blockchain technologies will ensure that chains of custody for evidence remain tamper-proof, while quantum computing will help to speed up complex analyses. At the most ethical level, such that AI is integrated responsibly into forensic science, it will be possible to improve already existing justice systems and public safety.[7]

In terms of forensic applications for AI, most can be summed up pretty easily, such as analyzing crime scenes, recognizing faces, evaluating DNA, and enabling cyber forensic evidence

[5] Houck MM, 'CSI: AI – The Potential for Artificial Intelligence in Forensic Science' *ISHI News* (n.d.) <https://www.ishinews.com/csi-ai-the-potential-for-artificial-intelligence-in-forensic-science/> accessed 12 February 2025

[6] 'Unveiling the Impact of Artificial Intelligence in Forensic Science' *Geeta University Blog* <https://blog.geetauniversity.edu.in/unveiling-the-impact-of-artificial-intelligence-in-forensic-science/> accessed 16 February 2025

[7] 'The Role of AI and Digital Forensics in Modern Policing' *Magnet Forensics Blog* <https://www.magnetforensics.com/blog/the-role-of-ai-and-digital-forensics-in-modern-policing/> accessed 16 February 2025

 ISSN: 2582-6433

recovery. Scan a crime scene with an AI-powered drone, perform facial recognition for speedy identification of suspects, and enhance biometrics using AI. In digital forensics, AI automates and speeds up evidence collection and analysis from digital devices. Moving forward, it seems that most of the future development of AI in forensic science will be in the collaborative hands of researchers, law enforcement, and AI developers. Where adopting AI in conjunction with blockchain technology would make chains of custody tamper-proof, quantum computing would speed up complicated processes. Most ethically, at the level of AI integration within forensic science, it will be possible to bolster existing justice systems and those of public safety.

DEEPFAKE AND FORENSICS

Deepfakes are the terms used for artificial intelligence (AI)-created digital content, typically in video, audio, or image form, which has been modified by deep learning so that it can change, replace, or superimpose the original material over new material in a convincing manner.[8] The term "deepfake" is derived from the combination of "deep learning" and "fake." Recently, deep learning has been used as a workhorse for the recognition of various image/video visuals such as various facial landmarks, facial expressions and emotions, lip synchronization, head pose and alignment, lighting and shading and content regulation.[9] While the manipulation of video and image content proliferates, there are many uploads of videos, photos, and news, on a daily basis, on social media platforms like YouTube, Twitter, Instagram, Facebook, TikTok, and Weibo. Many current studies are proposing deep learning-based AI models to detect deepfakes, face swaps, face re-enactment, facial synthetics, attribute manipulation, identity swaps, and image- or video-based manipulations.

Deepfake technology is a newly discovered aspect of artificial intelligence and machine learning, which can be used to create highly realistic and manipulated media. It typically uses methods such as "Generative Adversarial Networks or GANs" and "Convolutional Neural Networks or CNNs" to generate synthesized images, videos, and audios that could deceive most into thinking that they are real persons.[10]

[8] Coccomini DA, Messina N, Gennaro C and Falchi F, 'Combining EfficientNet and Vision Transformers for Video Deepfake Detection' in S Sclaroff, C Distante, M Leo, GM Farinella and F Tombari (eds), Image Analysis and Processing – ICIAP 2022 (Springer International Publishing 2022) 219-229.
[9] Anantrasirichai N and Bull D, 'Artificial Intelligence in the Creative Industries: A Review' (2022) 55(1) Artificial Intelligence Review 589.
[10] Abbas F and Taeihagh A, 'Unmasking Deepfakes: A Systematic Review of Deepfake Detection and Generation Techniques Using Artificial Intelligence' (2024) 252 Expert Systems with Applications 124260.

 ISSN: 2582-6433

METHODS

1. Face swapping method: This is an interesting point, because face swapping is also represented in the context of replacing a target image or video with a source face instead of the target face, retaining corresponding information about attributes such as pose, lighting, and expression. GAN-based techniques make use of Generative Adversarial Networks in order to understand the identity features of the source face and transfer them seamlessly to the target face. Specifically, FSGAN (Face Swapping GAN) is an architecture that relies on neither specific data from these people nor on any kind of training; it uses the extracted alignment based on facial landmarks and segmentation maps to derive the convincible face blend. Very recently diffusion models have gotten into face swapping, treating this problem as some inpainting task in which the missing face area must be filled with reference to what exists in the target face in terms of already existing facial features but acquiring the identity of the source face. HiFiFace applies 3D facial shape information to guide identity transfer during high-fidelity face swapping, although it is limited by the precision of the 3D models. Self-supervised face swapping is a model programmed to learn from what it itself generates in order to better transfer identity and CLIP-guided face swapping is when the CLIP model is used to extract cues about pose, expression, and lighting based on the target image to recreate images in a more faithful manner.
2. Face re-enactment: Face re-enactment is the transfer of facial movements and expressions of the "driver" face in a video/image to a "source" face, making the source face mimic the driver's expressions. FSGAN may also be adapted for face re-enactment, learning to deform the source face based on the driving face. Audio-guided face reenactment uses audio as the driver, generating a photorealistic face that simultaneously moves its mouth with expressions corresponding to the input audio. Iterative face reenactment becomes useful when there is a substantial difference in head pose from the source to the driver and reenactment is done in different steps so as to better preserve the identity and texture of the source face.
3. General image/video synthesis: The general domain of image and video synthesis includes all methodologies for using AI to create new visual contents from scratch. In this fight, Generative Adversarial Networks (GANs) provide the best framework, where a generator creates the content, and a discriminator distinguishes it from real data. On the contrary, diffusion models start somewhere in the middle with random noise and work retroactively toward the finished picture/video, thus producing outputs that are of

 ISSN: 2582-6433

somewhat high fidelity and photo-realistic quality. An autoencoder learns a compressed representation of an image or video that can be modified and decoded to create truly novel examples and is helpful in understanding the underlying structure of data and generating similar content.[11]

Deepfake technology poses serious challenges to the legal systems as it creates convincingly manipulated media, which creates the possibility for evidence to be compromised. Digital forensics thus serves to combat this challenge through advanced detection techniques such as multi-modal analysis, machine learning algorithms, and metadata examination which help identify inconsistencies and manipulations in audio, video, and images. As deepfakes evolve, it is essential for legal frameworks to adapt, incorporating forensic expertise and ethical considerations to ensure how evidence is admissible, safeguarding justice against the abuse of this technology from being misused. Legal professionals and digital forensic experts may be required to work together, creating complementary skills, while new developments in detection technology will further protect the legal system from increasingly sophisticated forms of digital manipulation.

DATA MANIPULATION

Data manipulation means unauthorized adjustments to, deletions of, or falsification of digital information that may compromise the integrity of said data with repercussions on the legal proceeding.[12] Data manipulation encompasses a range of actions aimed at altering or falsifying digital information, posing a significant challenge to data integrity and trustworthiness. These techniques include data alteration, where existing data is modified to misrepresent facts or conceal activities; data deletion, which involves removing files or data to hide evidence, often necessitating recovery techniques to retrieve the information; and data fabrication, the creation of false data to deceive or mislead, which can range from generating fake documents to fabricating entire datasets. Steganography, another critical manipulation method, involves hiding data within seemingly innocuous digital files or messages to conceal its existence, requiring specialized techniques like reverse steganography to uncover the hidden information. These diverse methods highlight the multifaceted nature of data manipulation, emphasizing the need for robust detection and prevention strategies.

[11] Abbas F and Taeihagh A, 'Unmasking Deepfakes: A Systematic Review of Deepfake Detection and Generation Techniques Using Artificial Intelligence' (2024) 252 Expert Systems with Applications 124260.
[12] Leppard Law Federal Criminal Defense Lawyers, 'Electronic Data Manipulation: Evolving Challenges in Digital Evidence Cases' Leppard Law <https://leppardlaw.com/federal/obstruction/electronic-data-manipulation-evolving-challenges-in-digital-evidence-cases/> accessed 15 February 2025

 ISSN: 2582-6433

Digital forensics is vital in investigating and discovering data manipulation, relying on a series of systematic processes to identify, collect, examine, and report on digital evidence. Investigations typically start as systematic investigations to identify places of possible evidence and secure the area to prevent any further changes. The next phase, acquisition, that includes collecting relevant digital evidence such as log files, hard drives, and network traffic data, is performed with specialized hardware and software tools to create identical copies of digital devices while ensuring that there is no alteration of data during collection. The examination phase consists of an analysis of the evidence collected, with the help of forensic tools to reconstruct events and ascertain signs of compromise, analyzing file metadata, recovering deleted data, and cross-drive analysis that looks for anomalies across different drives. Anomalies with ELA would suggest areas with manipulated compression inconsistency. Reverse steganography could also be another avenue exploited. The last stage of this forensic process focuses on the presentation of findings in a comprehensive report, complete with methodologies and conclusions, and providing, if need be, expert testimony in court.

Data manipulation greatly endangers the sanctity of legal proceedings in the digital arena, especially in federal obstruction of justice cases, where the very fabric of electronic evidence is at stake. Evidence of manipulation may vanquish one piece of evidence while compromising another, with the added disadvantage to prosecutions being the potential cause for an acquittal. The crux of the matter is intent: the fact that one did it could in itself constitute a defence, whereas an absence of corrupt motive may be its centrepiece. Practitioners should always be on the lookout; if they suspect any signs of data manipulation, these should create knees-up challenges for the admissibility of such digital evidence, in the interests of fair play and justice. The dynamic legal environment now requires the courts to evolve in terms of their understanding of digital evidence, placing increasing importance on proper data collection and preservation protocols.[13]

And on a bigger dimension, discuss manipulations of data whose ramifications or consequences could transcend a particular case and raise the question of the security of digital information vis-a-vis privacy issues. Finding the balance between the need to have some transparency in these aspects but also protect the information that is sensitive from constitutional protections in which an individual should be protected from possible abuses. Technical evidence

[13] Zenarmor, 'What is Digital Forensics in Cybersecurity?' Zenarmor <https://www.zenarmor.com/docs/network-security-tutorials/what-is-digital-forensics> accessed 15 February 2025

 ISSN: 2582-6433

increasingly fortifies against obstructive allegations, bustling legal teams that must keep their heads above the changing tide of disruption by digital data manipulation.[14]

ENCRYPTION

Encryption is the practice of securing data for use of a select few. In this process, some plaintext is transformed into an encoded text known as ciphertext, which can only be encoded and decoded using a public key: to an unauthorized user, this ciphertext will seem unrecognizable gibberish. This procedure becomes highly useful in dealing with sensitive information, and it is mostly utilized by government agencies, especially in areas such as national security, defense, or communications with embassies abroad. Cryptography, the science of encryption, dates back to the great ancient Roman and Greek civilizations. It traveled through various applications down the ages but the rise of systems and formation of a digital world in all corners of the world have made encryption unavoidable for the government as well as private organizations.[15]

Encryption is considered the cornerstone of data security in the modern world, playing a critical role in protecting information and safeguarding privacy. It converts readable data called plaintext into unreadable ciphertext to obscure sensitive information from unauthorized users. In simple terms, encryption secures plaintext, which confirms confidentiality and prevents unauthorized access to personal data, trade secrets, or private communications. It also ensures data integrity, which means data cannot be changed or interfered with during transmission or storage, especially important for financial transactions and medical records. In addition, encryption offers protection of personal and sensitive data for regulatory compliance with GDPR, HIPAA, and other standards, thus helping organizations avoid incurring potential penalties for non-compliance. Encryption represents a strong shield against cybercriminal activities, such as ransomware and malware, rendering stolen data worthless to hackers. The latest innovations in AI in encryption will use such intelligence to dynamically vary encryption parameters, optimize encryption algorithms in real-time, and tailor its data protection strategy to ever-dynamic security threats.[16]

[14] Leppard Law Federal Criminal Defense Lawyers, 'Electronic Data Manipulation: Evolving Challenges in Digital Evidence Cases' Leppard Law <https://leppardlaw.com/federal/obstruction/electronic-data-manipulation-evolving-challenges-in-digital-evidence-cases/> accessed 15 February 2025

[15] Rizvi S, 'Key Factors for Regulating Encryption Under Indian Cyber Law' iPleaders (17 October 2023) <https://blog.ipleaders.in/key-factors-for-regulating-encryption-under-indian-cyber-law/> accessed 15 February 2025

[16] IBM, 'Encryption' IBM Think <https://www.ibm.com/think/topics/encryption> accessed 6 February 2025

 ISSN: 2582-6433

The provided search results make it difficult to identify specifically the challenges that encryption presents for forensic investigations. The information that is available infers several inferences. By its very design, for encryption grants an opportunity for making data unreadable without having the correct key very aspect that makes forensic investigations arduous. Therefore accessing encrypted data entails some hindrance to the encryption imposed on it, and this would cost the investigation in time, effort, and funds rendering it impossible with the actual decryption key. These challenges could impede investigations and, therefore, render possible avenues of criminality undetectable. With encryption, data and activities may also be concealed from network monitoring systems and security tools.[17]

LEGISLATIVE FRAMEWORK

The EU's AI Act is the first regulatory effort to provide a common legal framework for AI in the EU. It went into effect on August 1, 2024, and will be implemented in stages for the months thereafter. The Act classifies AI applications into increasing levels of risk occupancy: unacceptable, high, limited, and minimal, with one other category specifically for general-purpose AI. Applications that pose an unacceptable risk, namely social score systems and manipulation of human behaviour by AI, are banned. Under the Act's regime, high-risk applications are made accountable to stringent requirements, an example of compliance is, security, transparency, and quality requirements encompassing assessments of conformity. Limited-risk applications shall be governed by lighter transparency obligations, such as informing users that they are interacting with AI. The regulation of minimal-risk applications is almost absent. On top of that, the Act requires general-purpose AI to have transparency requirements and extra assessments for models with high capabilities. In the interest of enforcing the law and ensuring cooperation, the EU AI Act creates new agencies: the AI Office and the European Artificial Intelligence Board. Non-compliance can entail hefty financial sanctions. The Act intends to strike a balance between nurturing innovation in AI and ensuring AI is developed in a responsible, ethical, and trustworthy manner, with appropriate protection of fundamental rights, thereby enhancing transparency.

Introduction to the Digital Personal Data Protection Rules (DPDP Rules), 2025-the document released by the Union Ministry of Electronics and Information Technology (MeitY) on January 3, 2025, under the Digital Personal Data Protection Act, 2023 entitles to the establishment of

[17] Cloudian, 'Data Encryption: The Ultimate Guide' Cloudian <https://cloudian.com/guides/data-protection/data-encryption-the-ultimate-guide/> accessed 10 February 2025

 ISSN: 2582-6433

safeguards for personal data to protect privacy rights. The draft will be open to public opinion until February 18, 2025, and has 22 clauses along with 7 schedules, supplementing the 44 sections of the DPDP Act.

As one of the exempted acts in the country, the DPDP Act will primarily focus on the establishment of legal comprehensive digital personal data protection laws in India, balancing the rights of individuals on the one hand to protect personal information while addressing the need of society and the legitimate purposes of processing data. It shall apply to the processing of digital personal data, which is collected online or offline but is digitized at the end of the process.

FEATURES

1. Notice requirement: It is important to provide an intelligible and adequate notice to data principals before the consignment of their personal data under India's DPDP Act. The language of the notice has to be English and all eight languages listed in the 8th Schedule of the Indian Constitution, as that would make the notice understandable to a large section of people. The notice must contain all categories of personal data collected and state their purpose in the utilization of the data. Moreover, the notice must explain how an individual may exercise his or her rights, including withdrawing consent and lodging complaints before the Data Protection Board. The DPDP Act further mandates that the data fiducial provide this privacy notice with every request for consent. Hence the consent is given only when an individual is made aware of the facts. The consent should be given freely with respect to the subject matter, given with full knowledge of the facts, and should consequently be given bearing in mind the rights of the data subject, with no conditions attached to the giving of such consent. Clarity of presentation and simple language is required, with multiple language delivery being provided by data fiduciaries. While the DPDP Act is cantered on consent, it provides for certain legitimate grounds for processing where consent need not have been obtained, albeit earlier versions of the DPDP contemplated inclusion of specific provisions on purpose limitation. In addition, individuals shall have the right to determine whether a certain fiduciary is or is not processing his/her data, to be provided with a summary of such data and processing activities, and to request a list of all data fiduciaries with which such data has been shared.

 ISSN: 2582-6433

2. Consent manager: Consent Managers, under India's Digital Personal Data Protection Act, are defined by the DPDP Act as those entities registered with the Data Protection Board to act as a central point for data principals to manage their consent. They provide the means for data processing consent to be given, managed, reviewed, and withdrawn through an accessible and transparent platform. This new framework strikes a balance between empowering individuals with autonomy over their personal data and enabling organizations with clear guidelines regarding data protection. Consent Managers stand out for the transparent, informed, and user-friendly mechanism related to obtaining and managing consent for data processing. Their work provides a legitimate basis upon which organizations can gain trust and respect from their users. They simplify the collection of consent via different channels, including websites or mobile applications or even retail outlets, wherein consent forms are simple, specific, comprehensible, and lawfully compliant. A consent manager manages secure record keeping and consent changes because that is needed in the first place for compliance. Timestamp records are created for each consent, thereby noting when, how, and for what purpose the consent was obtained. These independent entities manage data subjects' consent for sharing data through an interoperable, secure, and transparent platform. These managers ensure that the users have a readily accessible environment in which to view all consent given, denied, or withdrawn and consents with the attached notices and that this environment will facilitate easy withdrawal or modification of consents at any time by the user. Data through consent manager is end-to-end encrypted, transferred between the data fiduciary and the data user, and the consent manager has no visibility of the data.[18]
3. Data processing by the state: The DPDP Act intends to confer certain powers upon the State or its instrumentalities for personal data processing for the benefit or service provision to Data Principals. This would cover: (a) where the Data Principals have consented to the processing of their personal data for any benefits or services from the State or its instrumentalities, or (b) where such personal data is available in digital form, or in non-digital form and digitized subsequently, from any database or register, book, or other document maintained by the State or its instrumentalities. In effect, the DPDP Act overrules the consent of the individual, as far as it relates to the processing of personal data by the State for the purpose of providing any benefit, service, license, or

[18] Kakati A, ‘Consent Manager Framework under India’s Personal Data Protection Bill’ *International Association of Privacy Professionals* (16 December 2021) <https://iapp.org/news/a/consent-manager-framework-under-indias-personal-data-protection-bill> accessed 11 February 2025

 ISSN: 2582-6433

certificate, and it permits using that data for any other purpose. The DPDP Act also provides for the processing of personal data by the State or any of its instrumentalities to perform their functions under the law currently in force in India or in the interest of the sovereignty and integrity of India or security of the State. This act is devised with the intention of balancing the individual's right to secure his personal data with the needs of society for personal data. Then there are fears that the exemptions given to the government would allow sufficient leeway for government agencies to collect, process, and hold personal data unnecessarily and create 360-degree profiles for surveillance.[19]

4. Security safeguard: According to the Indian Digital Personal Data Protection Act, data fiduciaries are expected to put in place reasonable security safeguards to protect personal data under their custody, whether processed by them or a data processor. The maximum penalty under the DPDP Act for failure to take reasonably secure measures to safeguard personal data is as high as INR 250 Crores. Minimum data security standards have been prescribed by the Draft Rules under the DPDP Act. Examples of such measures include encrypting, obfuscating or masking personal data, or using virtual tokens. The draft also says that data fiduciaries must control access to resources of computers, maintain visibility on access in logs and monitoring to allow detection of unauthorized access, and back up data to continue processing in times of data compromise. Access logs must be kept for a year in case some study is to be done for detection, investigation, and prevention of unauthorized access unless a different period is specified by a law. A contract between a data fiduciary and a data processor should contain reasonable security safeguards with significant technical and organizational measures. A major data fiduciary will also be required to appoint an independent data auditor to do a periodic Data Protection Impact Assessments (DPIAs). Such assessments are used to determine the rights of data principals, the purpose of processing their data, and the management of risks to such rights.
5. Rights of data principles: Individual Data Principals, under the Indian Digital Personal Data Protection Act (DPDP Act), are endowed with many important rights for safeguarding their personal data. These rights empower individuals in controlling their information, as well as ensure transparency and accountability into the organization processing that information. Data Principals have the right to be informed concerning the processing of their personal data, i.e. the categories of data being processed, the

[19] PRS Legislative Research, 'Digital Personal Data Protection Bill, 2023' *PRSIndia* <https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023> accessed 11 February 2025

 ISSN: 2582-6433

purpose of processing, the source of the data and the details of who is processing the data. Another thing that Data Principals enjoys is the right to rectify personal data which is incomplete or inaccurate Furthermore, Data Principal has also the right to be forgotten. Wherein the Data Principal can ask the deletion of their personal data whenever such data is not necessary anymore for the stated purpose of processing or whenever Data Principal revokes his or her consent. In addition, Data Principals may exercise the right to restrict processing of their personal data in certain situations such as unsubscribing from mailing lists. They also have the right to data portability, enabling them to get their data in a structured format, commonly used and machine-readable format to transmit it to another data fiduciary. These rights include the right to object to the processing of their data for certain purposes including direct marketing or automated decision making. Lastly, the Data Principal is still empowered to withdraw their consent at any given point, thus keeping them in charge of processing their data. To exercise these rights, Data Principals must submit a written request to the data fiduciary, who must provide a response within 30 days. If the response fails to satisfy the Data Principal, he or she may approach the Data Protection Board of India with a complaint.[20]

6. Data protection impact assessments: Data Protection Impact Assessments (DPIAs) under the Indian Digital Personal Data Protection Act (DPDP Act) are fundamental. DPIA may be defined as a process, which consists in short, with a description of the rights of Data Principals and the purpose of processing their personal data. It also includes assessment and management of risks to the rights of Data Principals. The significant data fiduciaries shall appoint independent data auditor who undertakes periodic DPIAs. The Draft Rules specify that SDFs must undertake a DPIA and an audit, once within a 12-month period from the date of being notified as an SDF. The person performing the DPIA and the audit is required to furnish a report to the Data Protection Board containing significant observations. The assessment should also verify that the algorithmic software of SDF does not pose any risk to the rights of Data Principals. A DPIA is to evaluate and manage risks to data principals' rights. As per EY, organizations must be encouraged to perform DPIA for any high-risk processing activity. The same also states that even a Significant Data Fiduciary must conduct

[20] 'India DPDP Act Data Principal Rights and Requests' *Secure Privacy* <https://secureprivacy.ai/blog/india-dpdp-act-data-principal-rights-and-requests> accessed 11 February 2025

 ISSN: 2582-6433

DPIAs. DPIAs describe the rights of data principals, the purposes of personal data processing, and the assessment and management of risks to data principals' rights.[21]

7. Accountability and Compliance: Accountability and compliance are very basic principles in governance and organizational settings as far as regulatory frameworks and ethical business practices are concerned. Accountability is the duty of individuals or organizations to accept responsibility for the acts and decisions they make. This is a will to be transparent and answerable to stakeholders - employees, shareholders, and the community at large. In the corporate environment, accountability establishes the presence of mechanisms and systems needed for evaluating performance and behavior, therefore promoting a culture of responsibility that encourages ethical conduct and trust within the organization. In fact, both accountability and compliance are basic principles of governance and organizational setting in so far as the regulatory frameworks and ethical business practices are concerned. Accountability is the obligation of individuals or organizations to accept responsibility for the acts and decisions they make. This is a will to be transparent and answerable with respect to stakeholders - employees, shareholders, and the community at large. In a corporate environment, accountability is to put in place the necessary mechanisms and systems to evaluate performance and behaviour, which then fosters a culture of responsibility toward ethical behaviour and trust within the organization.

RECOMMENDATION

Firstly, a clear and effective operationalization framework for the Data Protection Board of India should be put in place. The workings of the Board must be made independent such that it can efficiently handle complaints and enforce compliance to the DPDP Act. Timely setting up of the Board with clear operational guidelines would inspire confidence in the regulatory framework, assuring individuals that they have a viable pathway for redressal in scenarios of data breach or personal data misusing.

Secondly, the SDFs should receive appropriate direction with respect to the added obligations that fall under the DPDP Act. This would include procedures for conducting DPIAs and obtaining other regular audits. The government should also consider providing workshops and

[21] 'Introduction to the India Digital Personal Data Protection Act (DPDP Act)' *Usercentrics* <https://usercentrics.com/knowledge-hub/india-digital-personal-data-protection-act-dpdpa/> accessed 12 February 2025

 ISSN: 2582-6433

other forms of training to foster their understanding of their obligations and putting in place the means to comply with these obligations.

There should also be sensitization programs enlightening people about their rights in terms of the DPDP Act. There are many citizens who do not know what rights they have on their personal data, such as how to access, correct, or delete it. Thus by increasing awareness, individuals will be able to know and exercise their rights better hence raising accountability of data fiduciaries.

In addition to this, it is very important to make the security safeguards provided in the DPDP Act exhaustive and adaptable to changing technological threats. Regular updating of security standards and practices will ensure that personal data continues to be protected against breaches and unauthorized processing. Adopting best practices that can be implemented by organizations to improve their data protection may also result from cooperation with cybersecurity experts.

Such consideration should ensure that continuing interaction will exist between parties, including - public authorities, businesses, civil society and technology experts-to continually evolve the regulatory framework. Collaborative interaction can assist in identifying both bottlenecks and encouragements towards effective implementation of the DPDP Act, further guaranteeing its relevance in a fast-changing digital landscape. Fostering such collaboration will help India evolve a balanced approach for privacy protection and innovation and growth in the digital economy.

CONCLUSION

In conclusion, this research emphasizes the most important new dimension: legislation like the EU AI Act and India's DPDP Act 2025, which will have a tremendous impact on the regulation of artificial intelligence and data protection. They are a part of this international effort aiming to implement a very well-defined code of responsible technology use, counterbalancing the need for innovation with the safeguarding of basic rights. The EU AI Act, with its risk-based classification and transparency requirements, sets an exemplary standard for AI governance that would perhaps become a benchmark for global regulations. In parallel, the DPDP Act 2025 in India endeavors to give individuals control over their personal data, thereby instituting a holistic framework pertaining to the protection of personal data and privacy rights in the

 ISSN: 2582-6433

country.

The legislative frameworks' effectiveness, of course, is contingent upon their implementation and enforcement. The recommendations of this study-for example, the establishment of independent regulatory authorities, provision of guidance to organizations, creation of public awareness, provision of adaptive security measures, and promotion of stakeholder dialogue-are therefore indispensable for ensuring that the goals of these legislations are actually achieved. Contrary to this, the Data Protection Board of India must be empowered to act as an independent authority, while organizations need to be trained on their compliance obligations with respect to Data Protection Impact Assessments (DPIAs). Public awareness campaigns geared at informing individuals of their rights are necessary, using technologies that address the ever-changing threats posed by new technological advancements. It is with an ongoing dialogue between stakeholders that the law can stay relevant and effective in this fast-moving digital environment.

The recommendations may benefit the EU and India by creating environments in which people can embrace AI and digital technologies, promote innovation, and protect individual rights. The balanced approach aims to sustain a digital economy from which society can benefit as a whole. Future continued research and adjustment of these frameworks will also be needed as the technology continues to advance, ensuring that all ethical considerations are kept forefront of technological development. This will keep citizens fully informed and involved while leaving the ultimate fate of these legislative frameworks to an insistence of collective will toward responsible innovation and protection for citizens' rights and freedoms in the digitally emerging society.