Artificial Intelligence and Data Privacy

Balancing Innovation and Security in the Digital Age

Artificial Intelligence and Data Privacy

Balancing Innovation and Security in the Digital Age

Edited by

Dr. Anjali Dixit
Sr. Associate Professor of Law,
SOL, Lingaya's Vidyapeeth
(Deemed to be University), Faridabad, Haryana
Visiting Professor, Department of Law
KAAF University College
Gomoa Fetteh, Kakraba-Kasoa,
Ghana (West Africa)

ABS Books
Delhi-110086

ISBN : ???
Copyright : Editors
Edition : 2025

Published by
ABS Books
Publisher and Exporter
B-21, Ved and Shiv Colony, Budh Vihar
Phase-2, Delhi - 110086
✆ : + 919999868875, +919999862475
✉ : absbooksindia@gmail.com
Website : www.absbooksindia.com

PRINTED AT
Trident Enterprises, Noida (UP)

Overseas Branches

ABS Books
Publisher and Exporter
Yucai Garden, Yuhua Yuxiu
Community, Chenggong District,
Kunming City, Yunnan Province
-650500
China

ABS Books
Publisher and Exporter
Microregion Alamedin-1
59-10 Bishek, Kyrgyz
Republic- 720083
kyrgyzstan

Artificial Intelligence and Data Privacy: Balancing Innovation and Security in the Digital Age
By : *Dr. Anjali Dixit*

Preface

In the dawn of the digital age, the interplay between artificial intelligence (AI) and data privacy has emerged as one of the most pressing issues of our time. As technology advances at an unprecedented pace, the challenge of balancing innovation with security has become a critical concern for policymakers, legal scholars, and the global community. The book ***Artificial Intelligence and Data Privacy: Balancing Innovation and Security in the Digital Age*** delves into this complex and multifaceted relationship, offering a comprehensive exploration of the legal, ethical, and practical dimensions of AI and data privacy.

This volume brings together contributions from a distinguished group of scholars and practitioners who provide valuable insights into various aspects of AI and data privacy. **Dr. Anjali Dixit**, Senior Associate Professor of Law at Lingaya's Vidyapeeth and Visiting Professor at KAAF University College, starts the discussion with her chapter on *AI, Machine Learning & Big Data Laws and Regulations 2024*. Her work offers a critical analysis of the evolving legal landscape surrounding AI and data privacy.

Professor (Dr.) Rohit P. Shabran, Director of the Institute of Legal Studies at Shri Ramswaroop Memorial University, addresses *Data Privacy vs. AI Innovation: India's Balancing Act*. His examination highlights the delicate equilibrium that India seeks to achieve between fostering technological innovation and safeguarding data privacy.

B Mathanachandiran and **Dr. Ratheesh Kumar V.V** from VISTAS, Chennai, explore the interplay of *Artificial Intelligence, Data Governance & Privacy*. Their insights contribute to a deeper understanding of how AI is reshaping data governance and privacy frameworks.

Dr. Madhuri Vijay Sarwade, Associate Professor at Tilak Maharashtra Vidyapeeth's Lokmanya Tilak Law College, presents her research on *Emerging Patterns in Cybercrime Affecting Online Transactions and Banking Frauds in India*. Her work sheds light on the growing challenges of cybercrime in the digital age.

Dr. Sangeeta Sharma examines *AI & Law and Its Role in Future Legal Practice*, providing a forward-looking perspective on how AI might influence legal practices and the legal profession.

Aparna Chandra and **Sonal Rao**, Ph.D. scholars, delve into the *Evolution and Challenges of Data Protection Laws in India: A Critical Analysis*. Their contributions provide a critical assessment of the development and challenges of data protection laws in the Indian context.

Prof. (Dr.) Aqueeda Khan investigates *Artificial Intelligence in the Criminal Justice System*, offering insights into how AI technologies are being integrated into criminal justice practices and their implications for fairness and efficiency.

Dr. Anita Yadav discusses *Digitalization as a Concern of Privacy: Emerging Issues and Legal Framework*, highlighting the evolving concerns related to digitalization and the corresponding legal responses.

Mrs. R. Vimala and **Shahana Parveen P P**, along with **Dr. Mahesh M M**, explore the implications of *Digital Consumer's Confidentiality* and the impacts of excessive digital device use, respectively. Their chapters emphasize the significance of maintaining consumer confidentiality and addressing the psychological effects of digital overuse.

Dr. Devyani Chatterji and **Dr. Sapna Saxena** provide perspectives on *Indian Government's Policies on Cyber Security* and *Globalization and New Trends of Crime*, offering a comprehensive view of the policy landscape and emerging global crime trends.

Ms. Neha Prajapati and **Dr. Gunjan Baheti**, along with **Ms. Vinit Raikwar**, address the *Difficulties of Protecting Individual Rights in Artificial Intelligence* and explore the intersection of AI and legal practice in banking and financial sectors.

Finally, **Dr. Aneesh V Pillai** and **Nandana Rajesh** contribute a chapter on *Privacy and Data Protection: A Human Rights Perspective*, emphasizing the fundamental human rights dimensions of data protection in the context of AI.

This book aims to foster a nuanced understanding of how AI technologies intersect with data privacy and to provide practical insights into creating a balanced approach that promotes innovation while ensuring robust security and privacy protections. We hope this volume serves as a valuable resource for academics, practitioners, policymakers, and anyone interested in navigating the complex terrain of artificial intelligence and data privacy in the digital age.

Contents

1.

AI, Machine Learning & Big Data Laws and Regulations 2024

*Dr. Anjali Dixit**

Introduction

India has seen remarkable digital transformation in recent years, greatly impacting multiple sectors including healthcare, finance, e-commerce, education and the like. This digitisation of the Indian economy has significantly augmented the demand for technologies such as Artificial Intelligence ("AI") and Machine Learning ("ML").

India's AI market size is projected to reach USD 5.47BN by the end of 2024 and USD 14.72BN by 2030. Acknowledging this potential of AL/ML in transforming the economy, the Indian Government has shown active interest in the development, adoption and promotion of AI and ML tools/technologies across multiple sectors, envisioning AI as a 'catalyst' and a 'kinetic enabler' for India's digital economy. Multiple

***Sr. Associate Professor of Law, SOL, Lingaya's Vidyapeeth (Deemed to be University), Faridabad, Haryana, Visiting Professor, Department of LawKAAF University College Gomoa Fetteh , Kakraba-Kasoa, Ghana (West Africa)**

policy interventions have been introduced to achieve this objective, some of which are summarised below.

AI Legislative Framework/Government Advisories

Presently, India does not have a legislative framework that expressly regulates the development and use of AI and ML tools/technologies. It is expected that this sector will be governed by the Digital India Act, which may be released for public consultation by July 2024. This law is expected to facilitate AI development by 'safeguarding' innovation in AI, ML and other emerging technologies. The Government of India has indicated that while it will support monetisation of AI/ML technology in India, this process should be regulated by specific compliances for high-risk use cases, including human intervention and oversight, and ethical use of AI/ML tools and technology.

In the meantime, the Ministry of Electronics and Information Technology ("MeitY") has issued advisories to 'intermediaries' and 'platforms' that develop and make available AI tools and/or technologies to Indian users, asking them to comply with additional requirements specific to AI tools, as part of the due diligence obligations imposed upon such 'intermediaries' under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules"), framed under the Information Technology Act, 2000. While these advisories do not have a legislative backing, it appears that the private sector is working with the Government to address their concerns, to the extent feasible.

- ***Advisory on Deep Fakes*:** On December 26, 2023, MeitY issued an advisory to all 'intermediaries' to address the growing concerns around the misinformation powered by AI deepfakes. This advisory urged social media platforms and other intermediaries to comply with the IT Rules, particularly regarding the identification and removal of prohibited content, including deepfakes that impersonate others or spread misleading information.
- ***Advisory on the use of AI Models/large Language Models ("LLMs")/Generative AI/Ssoftware or Algorithms*:** Subsequently, MeitY issued another advisory to 'intermediaries' and 'platforms', including 'significant and large platforms' on March 15, 2024 (an earlier version issued on March 1, 2024 was updated), recommending that they, *inter alia*:
    1. ensure compliance with content-related regulations prescribed under the IT Rules in relation to the use of AI

models/LLMs/generative AI/software/algorithms;

2. ensure that the use of AI models/LLMs/generative AI/ software/algorithms, do not permit any bias or discrimination, or threaten the integrity of the electoral process;
3. label the possible inherent fallibility or unreliability of the output generated from the AI models and implement a consent mechanism that explicitly informs users of the fact that the content is derived from an AI tool/technology; and
4. ensure that any synthetic creation, generation or modification of a text, audio, visual or audio-visual information, that can potentially result in creation of misinformation or deepfakes, is labelled or embedded with permanent unique metadata/ an identifier, such that the computer source and the user of such content can be identified.

This advisory is the first formal guidance issued by the Government of India, relating to the use and allowance of AI models and tools including generative AI and LLMs in India.

- ***Privacy Law Aspects*:** The Indian Government has recently enacted a new data privacy law, the Digital Personal Data Protection Act, 2023 ("DPDP Act"). The DPDP Act, among others, affixes varied obligations on data fiduciaries (a person who decides the purpose and means of processing personal data), including imposition of significant penalties (up to INR 250 crores) for personal data breaches. Additionally, the DPDP Act prescribes specific consent requirements for processing personal data and prohibits behavioural monitoring, profiling of, and targeted advertisements involving children. While the DPDP Act itself does not regulate AI, it will have indirect implications on the way AI systems are developed and deployed, particularly when they make use of personal data.

India's AI Policy Initiatives

When asked about the Indian Government's potential plans/ policies for the use of AI, the Minister of State for MeitY, Mr. Rajeev Chandrasekhar, stressed the importance of ensuring safety and trust in AI for all citizens. The Minister also spoke of the necessity of implementing rules and regulations that provide guardrails for ethical and safe use of AI.

- ***National Programme on AI and the National Strategy for AI (2018)*:** As a part of India's national programme on AI, NITI Aayog, India's public policy think tank, was tasked with the responsibility of formulating policies and rules for the development of AI in India. In 2018, NITI Aayog released the National Strategy for Artificial Intelligence #AIforAll ("NSAI 2018"),[6] which focused on leveraging AI for social and inclusive growth in line with the Government of India›s projected AI roadmap. The NSAI 2018 identified five sectors to benefit the most from AI: (i) healthcare; (ii) agriculture; (iii) education; (iv) smart cities and infrastructure; and (v) smart mobility and transportation.

The NSAI 2018 also launched 'AIRAWAT' (Artificial Intelligence Research, Analytics, and Knowledge Assimilation Platform) for promoting research and development of AI by facilitating collaboration among various stakeholders including academia, industry and Government agencies, to advance AI technologies and applications in India. 'AIRWAT' was recently ranked 75th in the top 500 global supercomputing list at the International Supercomputing Conference in Germany in 2023.

In February 2021, NITI Aayog published a set of principles outlining responsible AI practices. These principles emphasise the importance of ensuring safe, reliable, fair, transparent, accountable and inclusive AI systems. Recognising the potential societal impacts of AI technologies, these principles aim to guide policymakers, researchers and industry stakeholders in developing ethical and responsible AI solutions. Building upon these foundational principles, NITI Aayog further operationalised responsible AI practices in August 2021 by releasing guidelines for integrating these principles into real-world AI applications. These operationalising principles provided actionable steps and frameworks for incorporating ethical considerations and risk mitigation strategies throughout the AI development lifecycle, reinforcing India's commitment to fostering AI innovation while safeguarding against potential harms and ensuring societal well-being.

- ***Taskforce Report*:** The Ministry of Commerce and Industry also constituted a Task Force on Artificial Intelligence to submit a report on AI for economic transformation of India. The Task Force Report acknowledged that data is the bedrock of AI systems and reliability of AI systems depends primarily on quantity and quality of data. The Report assessed that it is crucial for AI

systems, among others, to:

1. have explainable and demonstrable behaviour;
2. have engineering for safety and security;
3. undergo an audit for non-contamination by human biases and prejudices; and
4. be transparent and comply with industrial standards.

The Task Force also required for legal provisions applicable to human users of AI systems to continue to apply, as relevant, to autonomous machines and called for specific liability provisions to be worked out for certain categories of machines.

- ***Draft National Data Governance Framework Policy* (*NDGFP*):** In May 2022, MeitY released the draft NDGFP with an aim to capitalise the full potential of digital governance by maximising data-led governance and data-based innovation. Further, the policy also launched the non-personal data-based India Datasets programme which outlined the methods and rules to be adopted by the Government and private entities to safely access non-personal data and anonymised data for research and innovation use cases. Among others, the NDGFP proposes to set up a Data Management Office responsible for framing, managing and periodically reviewing the policy, as well as design, and manage the India datasets platform that will process requests and provide access to non-personal and/or anonymised datasets.
- ***India AI 2023 Expert Group Report by MeitY*:** The seven expert working groups set-up by MeitY released their first edition of 'IndiaAI' in October 2023, which outlined comprehensive strategies for leveraging AI to propel India's growth and development. The report emphasises a holistic and ambitious approach, encompassing various aspects like research, development, skill, infrastructure and ethical considerations. Key recommendations include:
  1. Enhancing AI skill penetration: The report suggests ways to equip India's workforce with the necessary AI skills through targeted programmes and training.
  2. Strengthening AI computer infrastructure: It proposes public–private partnerships to bolster India as a destination for AI infrastructure and innovation.

By implementing these recommendations, India aims to become a global leader in responsible AI development and utilisation.

- ***Complex Adaptive System ("CAS") Framework to Regulate AI*:** The Economic Advisory Council to the Prime Minister of India ("EAC-PM") recently proposed a unique approach for regulating AI through a CAS framework. This CAS framework views AI as dynamic, unpredictable and one that cannot be regulated through traditional regulatory mechanisms, which typically rely on *ex ante* impact analysis and risk assessment. The CAS framework proposed by the EAC-PM will work on five key principles:
  1. establish guardrails/boundaries to ensure that AI technologies do not exceed their intended functions and to avoid a domino effect where a malfunction in one system cascades into a larger systemic failure;
  2. establish control through manual overrides to ensure human intervention when AI systems become unpredictable;
  3. ensure transparency by adopting open licensing for core algorithms, where external experts can conduct audits and assess AI systems for bias, privacy and security risks;
  4. ensure accountability by mandating standardised incident reporting protocols and establishing predefined liability protocols to ensure that entities or individuals are held accountable for AI-related malfunctions or unintended outcomes; and
  5. set-up a specialist regulator who can respond swiftly and ensure that governance remains proactive. Overall, the CAS framework offers an adaptable and effective approach for governing AI in India.

Sectoral Initiatives

- ***Telecom Sector*:** Recognising the transformative potential of AI, the Telecom Regulatory Authority of India ("TRAI") issued recommendations in July 2023 to shape responsible adoption of AI within the telecom sector. TRAI emphasises the need for telecom service providers to invest in AI and ML-driven solutions for network optimisation, predictive maintenance and personalised services, thereby improving the efficiency and reliability of telecom infrastructure.

TRAI envisages use of AL and ML, *inter alia*, for:

1. real-time network analysis and optimisation, which can help improve call quality and data speeds;
2. predicting potential network issues and enabling preventive maintenance, thereby minimising service disruptions;
3. offering personalised service based on individual user preferences and usage patterns;
4. identifying and blocking spam calls and messages, thereby protecting users from unwanted communication and potential scams; and analysing communication patterns to identify and prevent fraudulent activities associated with spam and phishing attempts. These recommendations also emphasise the importance of adopting a conducive ecosystem for AI innovation by promoting collaboration between telecom operators, technology service providers and research institutions, to facilitate knowledge sharing and capacity building in development and support of AI/ML applications.

- ***Agriculture Sector***: The Indian Government has recognised the application of AI and ML in the agriculture sector, particularly in areas of precision farming, agricultural drones and hopping systems, livestock monitoring, monitoring climate conditions, etc. Several Agri-Tech startups are developing AI-powered solutions for precision agriculture, supply chain management and market linkages.
- ***Healthcare Sector*:** The Indian Council of Medical Research has published guidelines that aim to tackle ethical concerns pertaining to the utilisation of AI in medical research and healthcare. These guidelines are directed at technology companies, healthcare practitioners and research organisations who seek to utilise health data for medical research and facilitate healthcare delivery using AI technology.

Additionally, the Government has also launched programs such as the National AI Portal for Healthcare, which serves as a central repository of AI-based healthcare applications, research and resources. This initiative facilitates knowledge-sharing and capacity building among healthcare providers, researchers and technology developers. Moreover, various Government-funded research institutions and academic centres are conducting research and development in AI-enabled healthcare technologies, focusing on areas such as medical imaging analysis, predictive analytics and telemedicine.

- ***Education Sector*:** The NSAI 2018 proposed several key initiatives for the education sector, such as to leverage AI for adaptive learning platforms that tailor content and cater to individual student needs, utilise AI-powered tutors and virtual assistants who can provide personalised feedback and support to students, etc. The Government has also established the National Educational Technology Forum ("NETF"), which aims to facilitate the integration of technology, including AI, into teaching and learning practices across all levels of education. NETF serves as a platform of collaboration for policymakers, educators, researchers and technology developers to explore innovative AI-driven solutions that enhance educational access, quality and equity.
- ***Finance Sector*:** AI and ML can have multiple uses in the finance/fintech space, such as for customer due diligence, credit assessment, customer onboarding, underwriting and risk assessment, fraud mitigation and detection, etc. In a speech delivered on December 22, 2023, the Reserve Bank of India ("RBI") Deputy Governor, Shri Rajeshwar Rao, spoke about the potential of AI in the financial space, while also warning regulated entities such as banks and non-banking financial companies ("NBFCs") of the risks and concerns associated with it.[17] RBI is also working on developing AI and ML systems that can help improve its regulatory oversight of banks and NBFCs.
- ***Bureau of Indian Standards ("BIS") Standards*:** India's Standards-setting statutory body, the BIS, is working on formulating Indian Standards for the use of AI. The BIS has also framed and notified standards for AI using ML and AI assessment of ML classification performance.[20] These standards have not yet been made mandatory.

Global Initiatives

As the lead chair of the Global Partnership on Artificial Intelligence ("GPAI") for 2024, India hosted the GPAI Summit this year. The Summit witnessed participation of 29 member countries and various international organisations, such as United Nations Educational, Scientific and Cultural Organization, World Economic Forum, World Bank, etc., experts in the fields of AI, industry and start-up veterans, AI practitioners, academicians, students and officials from Central and State Governments. Prime Minister Narendra Modi, during his inaugural speech, stressed the responsibility enshrined in each nation

for the responsible development of AI.

As a part of the Summit, all 29 member countries unanimously adopted the GPAI New Delhi Declaration ("Declaration"), which acknowledged their commitment to work towards safe, secure and trustworthy AI, including, as appropriate, through the development of relevant regulations, policies, standards and other initiatives. The Declaration also stressed the need to mitigate risks associated with misinformation and disinformation, unemployment, lack of transparency and fairness, protection of intellectual property ("IP") and personal data, and threats to human rights and democratic values. The member countries conveyed their support for India's intentions to promote collaborative AI for global partnership.

Ownership and Protection

Patent Protection

In India, the relevant statutory framework that could create legal rights (i.e. IP rights) over an AI algorithm or the output generated from AI algorithms is envisaged under the Patents Act, 1970 ("Patents Act") and the Copyright Act, 1957 ("Copyright Act").

The Patents Act permits patenting of any 'invention' that is capable of industrial application and has the following essential elements:

1. it is a technical advancement over the existing knowledge or has an economic significance, or both;
2. it should not be obvious to a person skilled in the art; and
3. it must have characters of novelty, non-obviousness and enablement.

As per the Patents Act, '*a mathematical or business process or computer program per se or algorithms*' are not 'inventions'. The phrase '*per se*' leaves some doubt that the software can be patented provided it contains all the elements of an invention discussed under (i) to (iii) above. Similarly, if the output from the AI algorithm is to be protected by a patent, such output will also need to satisfy the essential elements of an 'invention'. There have been successful patent applications for AI-based software inventions in the recent years, and guidance in this regard has been provided by the Patent Office from time to time.

Further to the above, the autonomous capacity of an AI system to create '*inventions*' without direct human involvement may complicate

the process of obtaining patents for AI-based innovations in India, since the application process may require demonstration of human ingenuity. For instance, under the Patents Act, an application for a patent can be made by a 'person' who is the 'true and first inventor' or the assignee of the person claiming to be the 'true and first inventor' or by the legal representative of the person who is entitled to make such an application. Even the definitions of a 'Patentee' and 'true and first inventor' include references to a 'person'. It accordingly appears that the Patents Act presently necessitates human involvement or a human inventor for an invention to be deemed eligible for a patent. However, the Parliamentary Standing Committee in the report titled 'Review of the Intellectual Property Rights; regime in India' has observed that: '*...the condition to have a human inventor for innovating computer related inventions (innovations by AI and machine learning) hinders the patenting of AI induced innovations in India. Therefore, there is a need to review the provisions of both the legislations on a priority basis*."

It is safe to presume that there is presently insufficient clarity on whether the algorithm-based originator of the AI algorithm from which the output has been generated can be recognised as the owner of the patent under the Patents Act.

Copyright Protection

The Copyright Act grants copyright protection, *inter alia*, to a literary work, which is defined to include computer programs. The term computer program is broadly defined and is likely to include the source code of an AI algorithm. However, to be eligible for copyright protection, such source code must meet the following criteria:

1. firstly, it must be original, which means it must originate from the author; and
2. secondly, the work must have a minimum level of creativity, rather than being solely the result of skill and labour.

Similarly, for securing copyright over the output created by an AI algorithm, the output needs to satisfy the essential elements stated above.

In India, it is possible for AI software/algorithms to obtain copyright protection under the Copyright Act, as computer programs are eligible for such protection. Under the Copyright Act, the author of the work is recognised as the first owner of the copyright. The term 'author' is defined in the context of computer-generated literary work as the

'person' who causes the work to be created. The courts in India have interpreted the reference to 'person' under the Copyright Act to mean a 'natural person'.

On the other hand, like similar developments on this issue in other jurisdictions, it is not possible to take a conclusive position on whether an AI-generated output will satisfy the test of originality mandated under the Copyright Act, given that many of the commonly-used AI tools, particularly generative AI applications, process information available in the public domain and create content, resulting in generation of an output that may infringe third-party copyright or closely mimic pre-existing works. In such cases, the output generated by AI applications may not meet the criteria of originality and/or minimum level of 'creativity' necessary for copyright protection. The fact that AI-generated outputs are not created by a 'natural person' and are unable to meet the 'author' standard prescribed under the Copyright Act will also make it challenging to register such computer programs for copyright protection.

Accordingly, akin to the Patents Act, the Copyright Act cannot presently grant legal protection to the output created by an AI algorithm, if the process is devoid of a human intervention. The 161st Parliamentary Standing Committee Report also concluded that the Patents Act and the Copyright Act lack the necessary provisions to effectively support authorship and ownership by AI.

In view of the above, there is currently no certainty or reliable examples of AI material securing adequate protection under the IP laws in India, which makes it necessary for appropriate legislative measures to be undertaken to align the IP rights regime with ownership/proprietary nuances specific to the AI sector, so that the growth of the sector can be insured.

Trade Secrets Protection

AI applications rely on multiple datasets to train their models. Some of such data may be considered as 'trade secrets' and entitled to protection under common law as well as the Copyright Act.

While there is no dedicated law in India that grants protection for trade secrets, and this term lacks a formal definition, trade secrets are commonly understood as non-publicly available information that has commercial value, and for which the rights holder has taken reasonable steps to protect – such as formulae, patterns, compilations, programs,

devices, methods, techniques or processes. Typically, such data is shared under a confidentiality agreement or is subject to confidentiality obligations. Examples of trade secrets include client lists, technical drawings, etc. Any use of trade secrets by a third party entitles the rights holder to remedies under the Copyright Act, contract laws, as well as under the common law applicable in India. It would therefore be important to consider a fact-specific assessment of the category of data that may qualify as a trade secret.

Antitrust and Competition Laws

AI-driven technologies are not only redefining market dynamics but also raising complex techno-legal and regulatory challenges. For instance, when AI-powered systems independently interact and exchange information, there is a risk of these machines coordinating strategies, leading to anti-competitive practices like self-preferencing, predatory pricing, rebates, tying and bundling, excessive pricing, unfair trading conditions or price discrimination. Among the above, the most crucial use of AI has been for developing pricing algorithms that observe the surge in sales at different pricing events and accordingly devise a pricing strategy that can be adopted by the organisations. Furthermore, AI pricing algorithms of organisations operating in the same market can collude by devising a pricing strategy that is based on competitor pricing, which effectively could result in a situation where market factors direct the pricing of competing products to be the same. These organisations can, in other words, achieve the effect of horizontal agreement without sharing any information with each other. Such practices have caught the interest of the anti-trust regulator in India. In January 2014, the Competition Commission of India ("CCI") investigated the allegations of collusion by airlines that had implemented a pricing algorithm to determine the pricing of tickets.

Since then, the surge in AI development has prompted a closer examination of competition and antitrust laws, and how they can be applied to the ongoing practices. To adapt the regulatory landscape to the effect of AI technologies, CCI is actively assessing the impact of AI on market dynamics and potential anti-trust concerns stemming from data access, algorithmic biases and the dominance of AI-driven companies.

In addition to the above initiatives, the Ministry of Corporate Affairs has constituted a Committee on Digital Competition Law ("CDCL"), which has been tasked to examine the need for a separate law to

regulate the competition in digital markets, and to effectively deal with challenges that are specific to the digital economy. CDCL issued a draft report on February 27, 2024, wherein CDCL has recommended, *inter alia*, the introduction of a Digital Competition Act ("DCA"), which will be an *ex ante* legislation and is proposed to be applicable to large digital enterprises. The objective of the DCA will be to prescribe measures to proactively monitor the conduct of large digital enterprises to ensure intervention by the regulator before anti-competitive conduct transpires. The approach, if finalised, may be similar to the Digital Markets Act in the European Union.

In this age of digitisation, organisations can access multiple sources to collect large volumes of diverse data, ranging from consumer behaviour to the pricing of goods. This diverse collation of data – Big Data – is being monetised to develop strategies for business growth and customer engagement. Expectedly, due to their existing presence in the market, dominant enterprises are at an advantage as they have an abundance of such Big Data at their disposal, which they can rely upon to disrupt a new entrant in the market.

Additionally, any organisation having Big Data can analyse the demand and supply of goods or services to influence the pricing of the products. Section 4 of the Competition Act, 2002, prohibits enterprises or groups from abusing a dominant position by limiting or restricting supply of goods or services, which could be extended to activities occurring in the digital economy. CCI is evaluating the market position of big tech companies and how they impact the competition in the market.

Board of Directors and Governance

A company acts through its Board of Directors ("BoD"), as the management and governance of the company is vested in its BoD. While Indian laws on corporate governance do not prohibit AI from assisting in decision-making functions of the BoD, whether AI can assume the role of the BoD and perform their duties is something that can be determined in the context of the fiduciary duties imposed upon directors in charge of running the affairs of the company.

The (Indian) Companies Act, 2013, contemplates a director appointed to the BoD to be a natural person. The fiduciary responsibilities of a director of a company include:

1. acting in good faith to promote the objects of the company for the benefit of its members and in the best interests of its stakeholders;
2. exercising duties with due and reasonable care, skill and diligence while exercising independent judgment;
3. a duty not to be involved in a situation in which he may have a direct or indirect interest that conflicts, or possibly may conflict, with the interest of the company; and (iv) to not achieve or attempt to achieve any undue gain or advantage, either to himself or to his relatives, partners or associates.

It is unlikely that AI and ML will completely replace BoD in the foreseeable future. While AI and ML technologies have demonstrated remarkable capabilities in data analysis, pattern recognition and predictive modelling, and can assist the BoD in making important decisions, they lack the understanding, ethical judgment and strategic vision that can be found in human board members. Moreover, the idea of primarily replacing human board members with AI and ML raises significant ethical, legal and societal concerns. Algorithms are influenced by the datasets on which they are trained, which can perpetuate biases and lead to unfair outcomes. Additionally, delegating crucial decisions to AI systems could undermine accountability and transparency, potentially eroding stakeholder trust. That said, AI and ML systems, when used accurately, can act as good support functionaries to the BoD. It is also important that companies implement these tools with the help of robust risk-management frameworks, that includes AI adoption policies, stakeholder roles, accountability and oversight mechanisms.

References

1. Market Statistics available at – https://www.statista.com/outlook/tmo/artificial-intelligence/india (as visited on 15.08.2024)
2. AI will be kinetic enabler of India's Digital Economy, make Governance smarter and more Data-led: MoS Rajeev Chandrasekhar – Press Release dated April 14, 2023, available at – https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1916645(as visited on 15.08.2024)
3. Digital India Dialogues held on September 3, 2023, available at – https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf (as visited on 15.08.2024)
4. MeitY issues advisory to all intermediaries to comply with existing IT rules – PIB Release, available at – https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542 (as visited on 15.08.2024)
5. Available at – https://sansad.in/getFile/loksabhaquestions/annex/1714/AU522.pdf?source=pqals (as visited on 15.08.2024)

6. National Strategy for Artificial Intelligence, 2018, available at – https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf (as visited on 16.08.2024)

7. Available at – https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1926942 (as visited on 16.08.2024)

8. Approach Document for India Part 1 – Principles for Responsible AI, available at – https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf (as visited on 16.08.2024)

9. Available at – https://psa.gov.in/CMS/web/sites/default/files/publication/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf (as visited on 16.08.2024)

10. Available at – https://www.meity.gov.in/writereaddata/files/National-Data-Governance-Framework-Policy.pdf(as visited on 16.08.2024)

11. IndiaAI 2023: Expert Group Report – First Edition, available at – https://www.meity.gov.in/writereaddata/files/IndiaAI-Expert-Group-Report-First-Edition.pdf(as visited on 16.08.2024)

12. Available at – https://eacpm.gov.in/wp-content/uploads/2024/01/EACPM_AI_WP-1.pdf(as visited on 16.08.2024)

13. TRAI Recommendations on Leveraging Artificial Intelligence and Big Data in Telecommunication Sector, available at – https://trai.gov.in/sites/default/files/Recommendation_20072023_0.pdf(as visited on 17.08.2024)

14. Internet of Things and Artificial Intelligence in Agriculture – PIB Release, available at – https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1885193 (as visited on 17.08.2024)

15. Available at – https://www.startupindia.gov.in/content/sih/en/bloglist/blogs/AgricultureStartups.html (as visited on 17.08.2024)

16. Available at – https://main.icmr.nic.in/sites/default/files/upload_documents/Ethical_Guidelines_AI_Healthcare_2023.pdf (as visited on 17.08.2024)

17. Innovations in Banking – The emerging role for Technology and AI (Remarks delivered virtually by Shri M. Rajeshwar Rao, Deputy Governor, Reserve Bank of India – December 22, 2023 – at the 106th Annual Conference of Indian Economic Association in Delhi), available at https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1400 (as visited on 17.08.2024)

18. RBI selects McKinsey and Company, Accenture Solutions to use AI, ML to improve regulatory supervision, available at – https://cfo.economictimes.indiatimes.com/news/rbi-selects-mckinsey-and-company-accenture-solutions-to-use-ai-ml-to-improve-regulatory-supervision/102708568(as visited on 17.08.2024)

19. Available at – https://www.services.bis.gov.in/php/BIS_2.0/dgdashboard/Published_Standards_new/standards?commttid=Mzg2&commttname=TElURCAzMA%3D%3D&aspect=&doe=&from=2022-07-21&to=2023-07-21(as

visited on 17.08.2024)

20. Available at – https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/knowyourstandards/Indian_standards/isdetails(as visited on 17.08.2024)

21. *Mariappan v. A.R. Safiullah*, (2008) 5 CTC 97; and FAQ 6, Page 2, available at – https://ipindia.gov.in/writereaddata/Portal/Images/pdf/Final_FREQUENTLY_ASKED_QUESTIONS_-PATENT.pdf(as visited on 17.08.2024)

22. *Can Artificial Intelligence (AI) Machine be Granted Inventorship in India?* – Journal of Intellectual Property Rights, available at – https://or.niscpr.res.in/index.php/JIPR/article/download/1268/309/3604#:~:text=Due%20to%20the%20significant%20investment,given%20the%20title%20of%20inventor(as visited on 17.08.2024)

23. Section 2(1)(p) of the Patents Act, 1970.

24. Section 2(1)(y) of the Patents Act, 1970.

25. Report available at – https://techcrunch.com/2023/08/30/chatgpt-maker-openai-accused-of-string-of-data-protection-breaches-in-gdpr-complaint-filed-by-privacy-researcher/?guccounter=1(as visited on 17.08.2024)

26. *Eastern Book Company v. D.B. Modak*, (2002) PTC 641.

27. *Tech Plus Media Private Ltd. v. Jyoti Jand*, (2014) 60 PTC 121, *Navigators Logistics Ltd. v. Kashif Qureshi & Ors*, 254 (2018) DLT 307.

28. Ref. Page 30 of the Report available at – https://files.lbr.cloud/public/2021-07/161_2021_7_15.pdf?VersionId=S01fCQEC5DzDqKNymsGgxal6YXmJbUwM(as visited on 18.08.2024)

29. AI and its Effects on Competition, blog available at – https://swiss-economics.ch/blog-en/items/ai-and-its-effects-on-competition.html#:~:text=The%20challenges%20interacting%20AI%20raises&text=In%20each%20case%2C%20different%20competitive,choice%20architecture%20for%20downstream%20firms (as visited on 18.08.2024)

30. Article available at – https://www.azbpartners.com/bank/pricing-algorithms-ccis-first-major-encounter-with-assessing-new-age-collusions (as visited on 19.08.2024)

31. Market Statistics available at – https://www.statista.com/outlook/tmo/artificial-intelligence/india (as visited on 19.08.2024)

32. Available at – https : // www. mca. gov. in/ bin/dms/getdocument?mds=gzGtvSkE3zIVhAuBe2pbow%253D%253D&type=open (as visited on 19.08.2024)

33. News report available at – https://inc42.com/buzz/cci-to-examine-big-techs-market-position-their-data-advantage (as visited on 19.08.2024)

34. Section 166 of Companies Act, 2013.

2.

Data Privacy vs. AI Innovation: India's Balancing Act

*Prof. (Dr.) Rohit P. Sabran**

Introduction

Imagine a world where AI algorithms predict your medical needs, personalize your education, and even manage your finances – all powered by your data. While this future holds immense promise, it raises critical questions about **data privacy**, especially in a country like India, where a comprehensive data protection framework is still under development.

Understanding the complex landscape of data privacy and AI in India can be overwhelming. To navigate this landscape with ease, this article is structured into clear sections. Each section delves into a specific aspect, providing key information and insights. From exploring the existing legal framework to examining the roles of various stakeholders, this comprehensive approach ensures a clear and well-organized journey through this critical topic.

***Director, Institute of Legal Studies, Shri Ramswaroop Memorial University, Lucknow.**

Artificial intelligence is ubiquitous these days, from those eerily precise music recommendations to robots operating vast factories. But here's the thing: all this remarkable AI technology relies on extensive datasets to make decisions. And this data includes our personal information!

The pressing question now is, how can we harness AI while safeguarding our data? Worry not, because this article will unveil the potential threats AI poses to data privacy.

The Data Dilemma

AI's data appetite is insatiable. The more information it consumes, the better it performs. However, this reliance raises concerns, as companies collect and analyze vast amounts of personal data, from online behavior to even biometric information.

India's Data Privacy Challenges

Challenge	Description	Source
AI's Data Hunger	As AI systems become more sophisticated, their need for vast amounts of data to function effectively grows. This raises concerns about the collection and use of personal data by companies.	N/A
Lack of Robust Law	India is currently drafting the Personal Data Protection Bill, but it has not yet been enacted. This regulatory gap leaves room for potential misuse of data in the context of developing AI technologies.	PRS Legislative Research (https://prsindia.org/billtrack)
Data Localization	Potential restrictions on cross-border data flows could hinder global AI development and innovation by limiting access to diverse datasets.	MeitY, Government of India (https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022)
Informed Consent	As AI systems become more complex, ensuring individuals truly understand how their data is being collected and used can be challenging, making it difficult to obtain truly informed consent.	Carnegie Endowment for International Peace (https://carnegieindia.org/)
Algorithmic Bias	AI algorithms can perpetuate biases present in the data they are trained on, leading to discriminatory outcomes, especially for vulnerable populations within India's diverse society.	Centre for Internet and Society (https://cis-india.org/)

Emerging Solutions

India is actively shaping its data privacy landscape, with:

- **The DPDP Bill**: This proposed law aims to protect individual data privacy, establish guidelines for data handling, and create a Data Protection Authority.
- **Sector-Specific Regulations**: The Reserve Bank of India (RBI) has established guidelines for data management and privacy in

the financial sector.

- **Increased Public Awareness**: The ongoing debate surrounding data privacy is raising public awareness about the importance of data protection.

Striking the Right Balance

India faces the challenge of fostering responsible AI innovation while safeguarding data privacy. Here are some crucial considerations:

- **Responsible AI Development**: Emphasize "privacy by design" and ethical AI principles, ensuring data privacy is an integral part of the AI development process.
- **Transparency and Accountability**: Businesses must be transparent about data collection, usage, and sharing practices, empowering individuals to make informed choices.
- **Strengthening Technological Safeguards**: Invest in robust data encryption, security protocols, and privacy-enhancing technologies.

Data Ownership: Who Owns Your Data?

Data ownership can lie with the individual generating the data, the device/service provider, or the entity processing the data. The DPDP Bill aims to provide more clarity on this issue in India.

India vs. the World: A Data Privacy Comparison

Aspect	India	European Union (GDPR)	USA
Overarching Law	DPDP Bill (not enacted)	Comprehensive GDPR	Sector-specific
Emphasis on Consent	Increasing with DPDP Bill	Core principle	Varies across sectors
Data Localization	Potential restrictions	Restrictions on transfers outside EU	Some restrictions, national security focus

Balancing Innovation and Regulation

Balancing these two forces is crucial. Privacy-enhancing technologies like federated learning and AI ethics frameworks can play a significant role in achieving this equilibrium.

The Global Data Landscape

- **Global Data Creation**: Estimated to reach 180 zettabytes by 2025 (Source: IDC)
- **India's Internet Users**: Over 850 million (Source: IBEF, 2023)
- **India's Data Privacy Concerns**: Over 70% of Indians are concerned about data privacy (Source: LocalCircles, 2022)

The Road Ahead

Speed of AI development, cross-border data flow challenges, enforcement of data protection laws, and public awareness remain key challenges along India's data privacy journey.

Navigating the Data Maze: India's Journey Towards Data Privacy

- **Thought-provoking Scenario:** In a world increasingly reliant on data, from personalized healthcare to smart cities, safeguarding individual information becomes paramount. This section delves into the current state of data privacy in India, exploring the current patchwork approach and the potential shift towards a more comprehensive framework with the proposed Digital Personal Data Protection Bill (DPDP).

A Patchwork Landscape: The Current State of Play

India's data privacy landscape currently resembles a **patchwork** of laws and guidelines. The **cornerstone** is the **Information Technology Act, 2000 (IT Act)**, which primarily focuses on **cybersecurity** rather than comprehensive data privacy. Additionally, **sector-specific regulations** exist for healthcare, finance, and telecommunications, but these often lack uniformity, leading to inconsistencies in data protection practices across different industries.

The DPDP Bill: A Beacon of Hope

The upcoming **Digital Personal Data Protection Bill (DPDP)** aims to rectify these shortcomings by establishing a **comprehensive data protection framework**. This bill aligns with international best practices, like the EU's GDPR, and includes key provisions such as:

- **Stronger User Rights:** Individuals gain greater control over their data through provisions for informed consent, data correction, portability, and the right to be forgotten.

- **Data Localization:** To enhance data sovereignty and security, the DPDP mandates storing and processing certain sensitive data within India's borders.
- **Data Protection Authority (DPA):** This independent body will oversee compliance, investigate data breaches, and impose penalties for non-compliance.
- **Data Processing Principles:** The DPDP outlines principles for lawful data processing, emphasizing purpose limitation, data minimization, and accountability.

Provision	Description
Stronger User Rights	Informed consent, data access & correction, portability, right to be forgotten.
Data Localization	Requirement for storing and processing certain sensitive data within India.
Data Protection Authority (DPA)	Overseeing compliance, investigating breaches, and imposing penalties.
Data Processing Principles	Lawful processing, purpose limitation, data minimization, accountability.

The Road Ahead: Challenges and Opportunities

While the DPDP Bill is a significant step forward, ensuring its effective implementation requires addressing some key challenges:

- **Collaboration:** Close cooperation between government, industry, and civil society is crucial.
- **Adaptability:** Keeping pace with technological advancements and evolving privacy concerns.

Conclusion

India's success in the AI era hinges on a comprehensive data protection framework, responsible AI development, and collaborative efforts from government, industry, academia, and civil society. By taking a proactive approach to data privacy, India can pave the way for a thriving AI ecosystem while upholding the fundamental right to privacy for its citizens and the global community.

The DPDP Bill holds the potential to usher in a new era of data protection in India, fostering greater **clarity, consistency, and accountability** in handling personal data. However, effective

implementation and continuous adaptation will be critical for India.

References

1. National Association of Software and Service Companies (NASSCOM), «Demystifying the Data Protection Bill: A Guide for Startups and SMEs» (2023)
2. World Economic Forum, "Global Risks Report 2023" (2023)
3. Carnegie Endowment for International Peace, "Data Privacy and Artificial Intelligence: A Comparative Analysis" (2023)
4. Organisation for Economic Co-operation and Development (OECD), "Policy Framework for Trustworthy AI" (2023)
5. NITI Aayog, "Mission Statement and Annual Report 2022-23" (2023)
6. Gartner, "Top Strategic Technology Trends for 2024" (2023)
7. Ministry of Electronics and Information Technology (MeitY), Government of India, "Digital India" website (accessed February 29, 2024)
8. NITI Aayog, "National Strategy for Artificial Intelligence" (2023)
9. UNESCO, "Recommendation on the Ethics of Artificial Intelligence" (2021)
10. Global Partnership on Artificial Intelligence (GPAI) website (accessed February 29, 2024)
11. Carnegie Endowment for International Peace, "Data Privacy and Artificial Intelligence: A Comparative Analysis" (2023)
12. OECD (Organisation for Economic Co-operation and Development), "Recommendation of the Council on Multi-stakeholder Dialogue on Internet Policy" (2016)
13. European Commission, "International Transfers of Personal Data" website (accessed February 29, 2024)
14. Office of the European Data Protection Supervisor (EDPS), "National Data Protection Authorities (DPAs)" website (accessed February 29, 2024)
15. National Conference of State Legislatures (NCSL), "State Privacy Laws" website (accessed February 29, 2024)
16. NITI Aayog, "Mission Statement and Annual Report 2023-24" (2024)
17. European Commission, "A European Strategy for Artificial Intelligence" (2020)

◆◆◆

3.

Artificial Intelligence, Data Governance & Privacy-An Analysis

B Mathanachandiran & Dr. Ratheesh Kumar***

Introduction

The rise of generative AI in late 2022 has posed issues for data governance and privacy. The usage of input and output data, as well as data quality and availability, have raised challenging challenges for AI model training. Specifically, how to protect the rights and interests of all parties involved, including the persons whose data are gathered, processed, and produced by these models and systems. Recent breakthroughs in neural networks and deep learning have led to larger, more powerful, more computationally costly AI models. In 2017, researchers announced "transformers" - a neural network design that paved the way for significant advancements in AI language models and generative AI. Open AI's Generative Pretrained Transformers (GPT) series is one example of a "foundation model," which is trained on enormous amounts of data and may be used to various downstream tasks. Advances in AI computing infrastructure, including graphics

***Assistant Professor, VISTAS, Chennai.**

***Associate Professor & HOD, VISTAS, Chennai.**

processing units (GPUs) and data quality, have driven technological advancements in machine learning. These factors are essential for producing AI algorithms, data, and computing resources (OECD, 2024)[1]. This review shows that, despite problems, AI's inventive, technological, and legal breakthroughs are mostly consistent with and can even support privacy and personal data protection regulations. By identifying risks and opportunities, linking current OECD Privacy Guidelines to AI Principles, Taking stock of national and regional activities, and presenting crucial policy considerations for the future, It advances the OECD's aim of helping implement the OECD AI Principles, the world's first. Intergovernmental AI norm, and the well-established OECD Privacy Guidelines, a flagship legal instrument serves as the foundation for global data protection regulations. One of the dominant themes is the importance of "explainability" of AI algorithms to ensure accuracy, fairness, and accountability. Experts also noted that AI increases demand for large data sets, which are critical to build AI systems that generate more accurate outputs, but also increase privacy-related risks. Furthermore, experts highlighted that most AI Principles refer to privacy in general terms but do not establish an explicit connection between the capabilities of AI and the nature of AI-specific privacy challenges, with the possible effect of shifting the focus away from privacy when it comes to AI.

Generative AI Promotes Collaboration on AI and Privacy

Coordination between the AI and privacy communities has long been recognized as necessary. Generative AI systems, such as language models, generate content (e.g., text) based on patterns in large amounts of training data, emphasizing the need for rapid action. Generative AI opens up new prospects in various fields, such as code development, creative arts, education, and healthcare (OECD, 2023). This technology poses both new and increased hazards, such as discrimination, polarization, unclear decision-making, and potential for societal control. The OECD's paper "Advancing accountability in AI: Governing and managing risks throughout the lifecycle for trustworthy AI" (OECD, 2023) raises awareness about the privacy and data protection challenges posed by AI systems, including generative AI. Advancements in technology have led to advanced generative AI systems that can be difficult to discern from human-generated content. The use of massive volumes of data, including personal information, to train AI models raises concerns

1. https://www.oecdilibrary.org/sites/a1689dc5en/1/3/2/index.htm1?itemId=/content/publication/a1689dc5en&_csp_=5cbbea11094afe4b75c96b4a3ec0bcd2&itemIGO=oecd&itemContentType=book.

about privacy and data protection. Generative AI introduces privacy problems throughout both the development and deployment phases. Developers commonly use publicly available sources for training data, which may involve personal information released online. Access to data does not necessarily imply free collection and usage for AI training. Personal data collected for AI training must adhere to privacy principles outlined in the OECD Privacy Guidelines and global data protection legislation. Concerns about lack of openness in data processing may contradict the "Openness Principle" in the OECD Privacy Guidelines and state regulations. Large language models in text-based generative AI technologies have the potential to acquire, use, and re-use personal data without consent (Hannah Brown, 2022).

Generative AI systems may conflict with individuals' rights to access, amend, and remove personal data (known as the "Individual Participation Principle"). Using personal data to train machine learning models might make it difficult to delete or rectify, as it may require more resources to retrain the model. Ensuring these rights in generative AI models can be challenging, especially when training material is unstructured and filtered from the internet. Autonomous self-learning algorithms may lose accuracy and dependability due to user interactions and feedback loops, perhaps leading to misleading content or misinformation. Privacy concerns come from the potential for inferences to expose personal information that has not been revealed by the subject or is incorrectly attributed to them. Misleading content might expose security vulnerabilities. If identifying and deleting specific data sets from an AI model is technically and logistically complex, making rectification impossible, should the entire AI model, including the personal data, be deleted? Currently, it is challenging to properly understand the risks and consequences of applying privacy regulations to AI models.

Real and Problem Threats of Ai System

The OECD has identified real and potential hazards connected with AI systems, especially generative AI, in its work streams. The dangers are stated below:

- The spread of misinformation on a broad scale, especially through manufactured content that people mistake for actual content.
- AI models may generate false responses or unlawful photos, including "fake nudes" for child sexual exploitation.
- Harmful bias and discrimination on an expanded scale

- ❖ Risks to privacy and data governance can occur at various levels, including training data, model level, data-model intersection, and human-AI interactions.
- ❖ Large models can be opaque and complex, posing challenges to transparency and explainability.
- ❖ The inability to challenge model outcomes; and,
- ❖ Privacy violations include the leaking or inferring of private information, among others.

G7 Round Table for Data Protection and Privacy Authorities

In June 2023, the G7 Roundtable of Data Protection and Privacy Authorities ("G7 DPA Roundtable") released a statement on generative AI.[2] listing key areas of concerns from a privacy and data protection perspective, which include:

- ❖ Legal authority to process personal information, including that of juveniles and children, for training models.
- ❖ Security measures are in place to prevent unauthorized access to personal information stored in the training database.
- ❖ Implemented mitigation and monitoring procedures to ensure accurate and non-discriminatory personal information generated by generative AI algorithms.
- ❖ Transparency measures enhance openness and explainability in the use of generative AI systems.
- ❖ Implement technical and organizational procedures to allow individuals affected by or engaging with these systems to exercise their rights, such as erasure or opting out of automated judgments.
- ❖ Implement accountability methods to ensure responsible behavior among AI supply chain actors.
- ❖ Limiting the acquisition of personal data to only what is necessary to complete the intended task.

2. G7 (2023), Roundtable of G7 Data Protection and Privacy Authorities Statement on Generative AI, https://www.ppc.go.jp/files/pdf/G7roundtable_202306_statement.pdf.

Resolution on Generative AI Systems by the Global Privacy Assembly

The 45th Session of the GPA expressed concerns about generative AI systems in a resolution on October 20, 2023 (GPA, 2023).[3] The GPA has endorsed data protection and privacy guidelines for generative AI systems, including:

- ❖ Lawful basis for processing;
- ❖ Purpose specification and use limitation;
- ❖ Data minimisation;
- ❖ Accuracy;
- ❖ Transparency;
- ❖ Security;
- ❖ Privacy by Design and Default;
- ❖ Rights of data subjects;
- ❖ Accountability.

The GPA highlighted the challenge of balancing privacy standards like as data minimization and purpose limitation with the widespread acquisition of training data for machine learning.

The Rise of Generative AI Highlights Need to the Intersection of AI and Privacy Rules

The privacy and data protection community's actions, as well as proposed AI regulations such as the EU AI Act, raise the question of how these frameworks will fit together. Proposed AI legislation will be implemented alongside established privacy and data protection rules and regulator enforcement actions. Co-regulatory initiatives can help prevent duplicating and overlapping obligations across regulatory regimes. The EU AI Act highlights the importance of clarifying the relationship between rules and the General Data Protection Regulation (GDPR). GDPR's protections against automated decision making (ADM) and profiling have been implemented by courts and regulators for years. These include transparency obligations, the fairness principle to prevent discrimination, and strict consent requirements for ADM cases (Barros Vale, 2022). Although examples from ADM jurisprudence can explain duties under the AI Act, they can also cause confusion for policymakers and lawmakers, leading to uncertainty about compliance.

3. GPA (2023), Resolution on Generative Artificial Intelligence Systems.

Small and medium-sized enterprises (SMEs) with minimal resources may struggle to grasp how AI interacts with data protection and privacy regulations. To properly utilize the potential of generative AI, training models require a large amount of diverse and relevant data. Increased data access improves AI model performance by allowing for iterative learning from instances. Having diverse and high-quality data, including precision, completeness, consistency, dependability, validity, and timeliness, is crucial for developing trustworthy algorithms and improving the performance of AI models. Smooth and efficient data flows are essential for AI models to work optimally, allowing for continual learning and improvement. To reduce bias in AI systems, it's crucial to get training data from multiple areas or countries. This is especially important for models utilized across borders. Concerns have been raised about the global adoption of barriers to cross-border data flows, including personal and non-personal data. This raises the risk of restricting access to specific regions or countries for the development of AI-driven tools. Data should be easily accessible for maximum impact. This involves improving coordination and facilitating data sharing between public and commercial sector organizations. The OECD Recommendation on Enhanced Access and Sharing of Data (OECD, 2021) addresses these aspects.

Mapping Existing Oecd Guidelines on Privacy and AI: Key Policy Considerartion

The OECD AI standards from the 2019 Recommendation on AI, updated in 2024, can be compared to the privacy standards outlined in the 1980 Privacy Guidelines, which were revised in 2013. The OECD AI principles fall into two categories: The OECD (2019) proposes five value-based principles for governments to develop trustworthy AI strategies and policies, as well as five recommendations for national policies to benefit societies through AI ecosystems. The OECD Privacy Guidelines serve as the foundation for this mapping endeavor, which focuses on privacy and data protection. The OECD Privacy Guidelines do not explicitly mention data minimization or automated decision-making rights, but their implementation by OECD members has elevated them to the forefront of privacy policy. The decision to incorporate privacy issues into the OECD AI Principles does not imply that one framework replaces another. To analyze privacy in AI systems, we used the OECD AI Principles as a starting point for comparisons. AI-related provisions in data protection laws, such as limitations on automated decision-making and privacy by design/default principles, should be considered when analyzing national frameworks.

The Oecd AI Recommendation Includes Five Values-Based Principles

The OECD AI Recommendation encourages the deployment of creative and trustworthy AI that upholds human rights, democratic principles, privacy, and data protection. The recommendation for AI offers a definition of an AI system, which is now utilized in AI frameworks around the world, such as The EU AI Act and the Council of Europe's Framework Convention on Artificial Intelligence, Human Rights Democracy and the Rule of Law. An AI system is defined as a machine-based system that uses input to generate outputs like forecasts, information, suggestions, or judgments that can impact physical or virtual surroundings. AI systems have varying levels of autonomy and adaptability after deployment (OECD, updated 2023).[4]

Key Terms and Conccpts: Privacy and Data Governance

The AI Principles emphasize the importance of coordinating between the AI and privacy communities on "privacy and data governance" principles. This aspect of human-centered values and fairness focuses on data protection and privacy issues (OECD, 2023).5 According to a previous OECD report, AI systems may create power and information asymmetries between employers, employees, firms, and citizens (OECD, 2023). Generative AI poses systemic dangers, including the creation of erroneous synthetic information that may influence people's preferences, attitudes, and behaviors. (Lorenz, Perset & Berryhill, 2023) The privacy community is shifting from focusing just on individual problems to considering the societal impact of processing large amounts of personal data through upcoming technologies (OECD, 2021). Coordination between AI and privacy policy groups can clarify the role of data protection and privacy legislation, as well as Privacy Enforcement Authorities, in addressing individual and communal problems caused by generative AI. The OECD Privacy Guidelines, as well as best practices among OECD members, guide current privacy and data protection procedures. The principles of data processing include lawfulness, purpose limitation, data minimization, accuracy, openness, security, privacy by design and default, data subjects' rights, including automated decision-making, and accountability. Building trustworthy AI involves trust in data acquisition, processing, use, safety, and transparency. Ensuring AI systems are legally compliant

4. OECD (Updated 2023), Definition of an AI System

5. OECD (2023), "Advancing accountability in AI: Governing and managing risks throughout the lifecycle for trustworthy AI", OECD Digital Economy Papers, No. 349, OECD Publishing, Paris, https://doi.org/10.1787/2448f04b-en.

throughout their lifecycle is a crucial step. Privacy and personal data protection policies typically require a "lawful basis" for data collection and processing. In Generative AI, the legal foundation known as "legitimate interests" is regarded the most appropriate, despite other legal grounds being available. AI developers, providers, and users must have a legitimate interest in developing or implementing a model, ensure that the data processing is necessary, and avoid disproportionate interference with data subjects' rights. Balancing AI and privacy interests can be challenging, necessitating stronger collaboration between the two communities. Privacy rules require processing only required personal data for the intended purpose. The notion of data minimization is implicit in the OECD Privacy Guidelines and stated in privacy regulations like the GDPR and the California Privacy Rights Act. AI business models, particularly those based on generative AI, rely on large volumes of data for efficient training. This technique may not align with the data minimization principle as it may not be able to predict which personal data the AI system will require. According to ICO (2023), data minimization does not imply avoiding processing personal data or decreasing its bulk. When applying this idea, it's important to consider the specific AI system and aims. To properly contextualize data, it's important to specify its intended use before and throughout collection (OECD, 2023) This entails not only adhering to statutory standards, such as informing data subjects of their purpose, but also contemplating how to comply with them. Less data could be used to achieve the same objectives. In the context of AI, data minimization may mean Prioritizing data quality above quantity allows for more effective results. For instance, determining whether the AI, A model can be trained without using sensitive personal data by utilizing an existing public data source. Training data quality is more important than quantity when determining model accuracy. OECD (2023) suggests many strategies for developing AI systems that handle just necessary data and meet performance criteria. Widder (2023) proposes making AI model training data publically accessible, enabling scientific review and creation of less data-intensive algorithms. PEAs are critical for comprehending and guiding privacy considerations in AI. Integrating privacy ideas like the purpose definition principle with AI's unique features is especially important. The CNIL's practical guidance ("AI how-to sheets") help organizations establish the purpose(s) of AI systems in accordance with EU GDPR, while also taking into account the unique development process. According to CNIL (2023), if the purpose in the deployment phase is specified, explicit, and justified, it is assumed that the purpose in the development phase will also meet

these criteria. AI systems, particularly general-purpose models, may not have evident operational application throughout development. The objective of developmental processing is considered decided, explicit, and justified only when it is sufficiently precise. The CNIL rules provide examples of when a purpose is sufficiently defined. (CNIL, 2023).

Key Term Include Human Rights and Democratic Values

Human rights encompass civil and political rights such as equality, non-discrimination, freedom of expression and association, privacy, and economic, social, and cultural rights including education and health (OECD, 2023, p. 31).[6] AI can improve access to healthcare and assistive technologies for people with disabilities, but it can also disrupt power dynamics and polarize opinions at scale (OECD, 2023). Generative AI poses dangers, including the potential to manipulate public opinion through deceptive synthetic content (OECD, 20237; OECD, 20238). Additional human rights impacts include:

- ❖ Effects on human agency and self-determination (OECD, 2022)
- ❖ Impacts on freedom of opinion, expression, non-discrimination, assumption of innocence, and fair trial (OECD, 2022).
- ❖ Impacts on access to important services like education, healthcare, and banking (OECD, 2022).
- ❖ Impacts and negative externalities for vulnerable populations, including children and underprivileged groups (OECD, 2023)
- ❖ Power and information asymmetries (OECD, 2023)

Numerous non-privacy laws normally provide guarantees for these human rights. Privacy and data protection laws, as well as privacy risk assessments, are integral to human rights. Violations of the right to privacy can lead to violations of other human rights, which must be considered (OECD, 2023). The AI community increasingly relies on Human Rights Impact Assessments (HRIAs) (OECD, 2023). The privacy community relies on "Privacy Risk Assessments" (OECD, 2023) and "Privacy Impact Assessments" (GPA, 2023). The Chapter

6. OECD (2023), "Advancing accountability in AI: Governing and managing risks throughout the lifecycle for trustworthy AI", OECD Digital Economy Papers, No. 349, OECD Publishing, Paris, https://doi.org/10.1787/2448f04b-en.

7. OECD (2023), "AI language models: Technological, socio-economic and policy considerations", OECD Digital Economy Papers, No. 352, OECD Publishing, Paris, https://doi.org/10.1787/13d38f92-en.

8. OECD (2023), "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, https://doi.org/10.1787/bf121be4- **en**

on Accountability of the OECD Privacy Guidelines Implementation Guidance addresses concerns such as eligibility for rights, psychological manipulation, and impact on vulnerable populations (OECD, 2023). Courts and PEAs evaluate the impact of AI systems on privacy rights to ensure they are fair, lawful, and proportionate, in accordance with existing laws and regulations. Courts and PEAs balance the impact on privacy rights against the social benefits of employing AI systems. The CJEU Quadrature du Net case (Joined Cases C-511/18, C-512/18, and C-520/18) provides a detailed analysis of how the right to public security should be balanced against privacy rights in the context of algorithmic systems used to detect terrorist threats. And the Ligue des Droits Humains case (Case C-817/19). The CJEU provided guidance on allowing interference with privacy and freedom of expression to protect against terrorism risks. They also recommended specific risk mitigation measures, such as human control, for any system deployment. The Court's analysis was based on GDPR and the EU Charter's proportionality criteria.

Explainability and Interpretability

Policy discussions in AI and privacy include explainability and interpretability. The intricacy and frequently "black box" nature of machine learning-based AI systems, and These challenges are becoming more pressing, particularly as generative AI models emerge. Not simply black boxChallenges prohibit consumers from comprehending why a huge model makes erroneous statements or "hallucinations"(OECD, 2023). Model opacity can limit users' and designers' ability to comprehend and regulate unanticipated behavior, posing considerable hazards, including "existential risks" (Lorenz, Perset, & Berryhill, 2023). Data scientists are actively researching ways to make black box machine learning models more explainable while maintaining performance. Experts in human-computer interface (HCI) study how explanations affect people with cognitive disabilities. The US National Institute of Standards and Technology (NIST) created four principles for explainable AI, which serve as core qualities for such systems. NIST recommends that explainable AI systems: (i) provide evidence or reasons for outcomes and processes ("explanation"); (ii) be meaningful to individual users ("meaningful"); (iii) accurately reflect the system's process for generating output ("explanation accuracy"); and (iv) only operate under designed conditions and with sufficient confidence in its output,(NIST, 2021). The privacy community emphasizes AI explainability to ensure accurate, fair, and accountable data processing. Privacy and data protection legislation, as well as PEAs, define "transparency" as the explainability

and interpretability of data processing activities. Explainability may be required by courts and PEAs for algorithmic choices that affect individuals, as it ensures human oversight and allows for meaningful remedy (CJEU, 2022). Transparency is recognized as the most effective way to ensure supervision and accountability under modern privacy regulations. Some argue that "privacy requires transparency" (Rotenberg, 2021, p. 497). i.e., the protection of individual privacy might depend on systems and processes being open and transparent. There are many legal requirements for some sort of explainability (Maxwell and Dumas, 2023). Some requirements stem from privacy and data protection regulations, while others come from fundamental rights texts or constitutional provisions that ensure due process. There is a connection between explainability, human rights, and fairness. Data protection regulation does not cover all aspects of explainability and interpretation. Data protection regulations may not prioritize explainability and interpretability to assist data scientists in improving models or identifying safety hazards. PEAs analyze the explainability and interpretability of data processing techniques to assist individuals affected by algorithms in challenging their decisions or system operators in detecting potential discrimination in the algorithm's output. In cases of automated decision-making or profiling under Article 22 GDPR, the Spanish Data Protection Agency (AEPD) emphasizes the need for data subjects to understand how their information will be processed, including the use of AI and relevant logic. The AEPD warns that providing technical references for algorithm implementation can be confusing and contribute to information fatigue. Provide sufficient and easily accessible information to help subjects comprehend the processing behavior. The AEPD's handbook on AI-based data processing (AEPD, 2020) provides examples of important information for data subjects, however the application of these criteria depends on the type of AI component utilized:

Provide more information on the data used for decision-making, including its term of usage (e.g. age).

The relative priority or weight assigned to each data point in the decision-making

Quality of the training data and the sort of models utilized.

Profiling actions and their effects.

Calculate error or precision numbers based on the metrics used to assess the correctness of the inference.

The presence or absence of appropriate human supervision.

Refers to audits, specifically on potential deviations in inference results, and certifications for the AI system. The most recent audit completed on adaptive or evolutionary systems.

If the [AI] system incorporates information about identifiable third parties, it is prohibited to process such information without proper authorization and the repercussions of doing so.

Accountability

Both privacy and AI communities have created strategies for managing accountability and risks. Accountability and risk management have their origins in regulating complex systems like offshore drilling and financial services (Yeung, Howes, & Pogrebna, 2020).[9] Environmental protection law requires impact evaluations. Corporate compliance procedures aim to avoid illegal activity by workers and subcontractors, such as corruption and competition law violations, which contribute to accountability. Both groups are spending heavily in ensuring good risk management for AI systems, especially those that exploit personal data. The OECD's WPDGP and WPAIGO accountability frameworks can be linked to address AI governance issues. Both communities are investing heavily in effective risk management techniques for AI systems, especially those that handle personal data. The OECD's accountability frameworks, WPDGP and WPAIGO, can be linked to improve AI governance. The OECD's AI classification and accountability framework helps identify risks, stakeholders, and mitigation strategies for AI systems throughout their lifecycle. OECD Guidelines for Multinational Enterprises can help promote ethical business practice. The OECD's work on accountability builds on the OECD Privacy Guidelines, providing a framework for privacy risk management that is not AI-specific and aligns with the Guidelines' approach. To bridge the gap between AI and privacy, the OECD AI lifecycle framework and relevant legislation and regulations, such as the EU AI Act, should be considered. Legislative attempts are underway to include privacy and data governance into AI accountability frameworks. The EU AI Act establishes quality criteria for datasets used in AI model training, including identifying gaps and biases that could undermine human rights.

9. Yeung, K., A. Howes and G. Pogrebna (2020), AI Governance by Human Rights–Centered Design,Deliberation, and Oversight, Oxford University Press, https://doi.org/10.1093/oxfordhb/9780190067397.013.5.

International Responses From Private Enforcement Agencies

PEAs collaborate on responding to AI, including generative AI, through statements and resolutions:

- Statement on Generative AI by the DPAs of G7 countries, adopted on June 21, 2023.
- Resolution by the Global Privacy Assembly on Generative AI (Global Privacy Assembly, 2023)
- The GPA's International Enforcement Working Group (IEWG) issued a statement regarding web scraping in 2023.
- The Global Privacy Assembly adopted a resolution on AI and employment in 2023.

Privacy Enforcement Authorities Provide Guidance on How Privacy Law Apply To AI

PEAs have undertaken programs and issued recommendations on the use of AI technology, particularly generative AI tools, based on observations from regulatory sandbox experiments. In December 2023, Canadian privacy regulators established rules for ethical generative AI research and usage (Office of the Privacy Commissioner of Canada, 2023). The federal, provincial, and territorial privacy authorities collaborated to establish guidelines for developing, producing, and using generative AI models, tools, goods, and services that adhere to important privacy standards.

In January 2023, France's CNIL established an AI department to enhance its knowledge of these systems and address privacy threats, in preparation for the EU AI Act. On May 16, 2023, the CNIL issued an action plan for deploying AI systems that respect persons' privacy. The CNIL's action plan aims to facilitate the implementation of AI systems that protect persons' privacy, building on earlier work in this domain (CNIL, 2023).

The Spanish Data Protection Agency (AEPD) provided recommendations on GDPR compliance for AI-integrated operations (AEPD, 2020). The AEPD has provided additional recommendations, such as a comparison of transparency concepts in the EU AI Act and GDPR (AEPD, 2023).

The Ibero-American Data Protection Network has issued General Recommendations for Processing Personal Data in Artificial Intelligence (Ibero-American Data Protection Network, 2020).

The Republic of Türkiye's Personal Data Protection Authority (KVKK) produced "Guidelines on the Protection of Personal Data in the Field of Artificial Intelligence" after reviewing significant international resources, including the OECD AI Principles. This AI-specific guide offers advice for developers, manufacturers, service providers, and decision-makers to safeguard personal data in line with Law No. 6698 on the Protection of Personal Data.

The UK's Information Commissioner's Office (ICO) updated its guidance on AI and data protection on March 15, 2023. This section is expanded with particular recommendations for justifying judgments made by AI (ICO, 2020). On January 15, 2024, the ICO opened a consultation series on applying data protection law to the development and use of generative AI models. The UK GDPR requires developers to comply with data subject rights, accuracy principles, and lawful online scraping for training generative AI models.

The FTC has issued recommendations on using algorithms for automated decision-making. The blog article "Using Artificial Intelligence and Algorithms" discussed the benefits and risks of advanced technology, especially in AI and healthcare (FTC, 2020). The FTC's blog article on Truth, Fairness, and Equity in AI discusses how current US rules can prohibit biased or unjust AI use (FTC, 2021). On April 25, 2023, the FTC and three other federal agencies (Consumer Financial Protection Bureau, Justice Department's Civil Rights Division, and Equal Employment Opportunity Commission) signed a joint statement to combat discrimination and bias in automated systems (FTC, 20230).

Singapore's Personal Data Protection Commission has issued Advisory Guidelines regarding the use of personal data in AI Recommendation and Decision Systems. The Advisory Guidelines aim to clarify the use of personal data for AI training and development, provide consumer consent information, guide third-party AI developers, and support businesses in complying with the Personal Data Protection Act (PDPC, 2022).

Pea Enforcement Action in AI, Including Generative AI

PEAs have initiated enforcement measures related to AI and privacy, including against generative AI. Such efforts have mostly focused on OpenAI, the provider of ChatGPT.

On April 4, 2023, the Federal Office of the Privacy Commissioner (OPC) of Canada opened an inquiry into ChatGPT after receiving

a complaint about the service processing personal data without authorization. On May 25, the OPC announced a joint investigation into ChatGPT with the provincial privacy authorities of British Columbia, Quebec, and Alberta. The investigation will also examine OpenAI's compliance with openness, transparency, access, accuracy, accountability, and purpose limitation.

On March 30, 2023, the Italian PEA (Garante) issued an emergency ruling prohibiting OpenAI from handling personal data in Italy. The Garante identified probable GDPR violations related to lawfulness, transparency, data subject rights, processing of children's personal data, and data protection by design and default. A month later, the prohibition was lifted after OpenAI met the Garante's requirements for revisions.

On June 1, 2023, Japan's Personal Information Protection Commission (PPC) issued a warning to OpenAI. The warning stated that OpenAI should obtain consent before collecting sensitive personal data from ChatGPT users or other individuals. Additionally, OpenAI should provide notice in Japanese about the purpose of personal data collection for both users and non-users.

On July 27, 2023, the Personal Information Protection Commission of Korea (PIPC) levied an administrative fine of 3.6 million KRW (about USD 3,000) against OpenAI for failing to notice a data breach during the payment procedure. The PIPC identified non-compliance with the Personal Information Protection Act (PIPA) in areas such as transparency, lawful grounds for processing (without consent), controller-processor relationship clarity, and parental consent for children under 14. The PIPC has given OpenAI until September 15, 2023 to comply with personal data processing regulations.

In May 2022, Clearview AI Inc. was fined GBP 7,552,800 by the ICO for utilizing photographs from the web and social media to construct a global database for facial recognition purposes. The ICO ordered the corporation to stop collecting and utilizing publicly available personal data of UK residents and remove it from their systems. Clearview AI filed an appeal against both notices issued by the ICO. On October 17, 2023, the first-tier tribunal (FTT) agreed with the ICO that Clearview AI used billions of facial photos to track individuals' behavior and process personal information. Foreign subscribers could access and analyze the photographs using AI. The FTT held that the ICO could not enforce Clearview AI because its clients were limited to foreign law enforcement

and government agencies performing criminal or national security duties, which are not covered by the GDPR or UK GDPR. In November 2023, the UK Information Commissioner requested permission to appeal the Clearview AI verdict by the First Tier Tribunal (Information Rights). In October 2023, the ICO filed a preliminary enforcement notice against Snap Inc., the parent firm of Snapchat, for failing to properly examine the privacy risks posed by their generative AI chatbot 'My AI', particularly for children aged 13-17.

On July 27, 2023, the Brazilian PEA initiated an investigation into ChatGPT's compliance with the Lei Geral de Proteção de Dados (LGPD) following a complaint and media reports that the service is not in line with the country's data protection laws.

On April 13, 2023, the European Union will "foster co-operation and exchange information" for addressing complaints and inquiries into OpenAI and ChatGPT. On May 2024, the EDPB issued a report describing efforts and preliminary findings on specific elements of the study. The preliminary Opinions examine ChatGPT's compliance with important GDPR standards, including lawfulness and fairness. Transparency, data accuracy, and data subjects' rights (EDPB, 2024)[10]

Conclusion

This paper highlights opportunities for collaboration between the AI and privacy communities in the OECD and beyond, with a focus on developing resources and tools for trustworthy and privacy-friendly AI systems. This document identifies policy possibilities and problems relevant to these communities, as well as areas of complementarity and gaps. The OECD is using its unique cooperation infrastructure to promote a positive and proactive message on AI and privacy. The OECD. AI Expert Group on AI, Data, and Privacy, established in early 2024, aims to enhance collaboration between the AI and privacy communities through study. This includes developing guidance and suggestions for worldwide interoperability in AI and privacy governance. The Expert Group may collaborate with relevant specialists at the OECD and outside to address sector-specific concerns related to AI and privacy, such as in health, employment, and finance. In the medium run, collaboration activities can inform if AI and Privacy Recommendations need to be updated to reflect synergies across the groups. The newly formed expert group may generate useful tools for AI actors, privacy regulators, and data protection practitioners. International cooperation on AI and

10. EDPB (2024), Report of the work undertaken by the ChatGPT Taskforce, https://www.edpb.europa.eu/system/files/202405/edpb_20240523_report_chatgpt_taskforce_en.pdf.

privacy should prioritize the long-term interoperability of relevant legal, technical, and operational frameworks. This enables policymakers to find commonalities, complementarities, and convergence in their individual frameworks, as well as stumbling blocks that may inhibit collaboration.

◆ ◆ ◆

4.

Emerging Patterns in Cybercrime Affecting online Transactions and Banking Frauds in India

*Dr. Madhuri V. Sarwade**

Introduction

With the increase in internet, the whole world has become a global village wherein everything is easily accessible. Technology has made international communications and interaction easier and quicker. A business in Tokyo can find a supplier in Mexico City trough a quick series of searches on the internet. An agreement might be stuck in a short period of time through the exchange of order forms through e-mail communications. Travelling might not be necessary at all. This has lead to an increase in the number of internet transactions[1]. Considering the current situation and circumstances internet has become an indispensable part of our daily lives.[2]

1. Indian Bar Review. Vol. XLI (2) 2014.p.181-182.
2. Ibid 182.

*Associate Professor in Tilak Maharashtra Vidyapeeth's Lokmanya Tilak Law College, Mukundnagar, Gultekdi, Pune. Maharashtra.

"Google knows quite a lot about all of us. No one ever lies to a search engine. I used to say that Google knows more about me than my wife does, but that doesn't go far enough. Google knows me even better because Google has perfect memory in a way that people don't".

– Bruce Schneier, Cyber Security Expert[3].

With the technological advancement almost all the information is now being stored in electronic media. Easy storage features and the reduced cost of storage media have created paperless offices, which are more efficient in discharging their functions. Computer technologies also have proliferated into the economic sectors (Banking and Insurance), social sectors (police help- lines, Academic and scientific research) health and other agencies[4].

India's Digital Banking Landscape

The banking industry has enjoyed the ride of emerging technology to undergo significant changes. Banks are among the biggest beneficiaries of the IT revolution and have largely adopted IT solutions for rendering the banking services to their customers[5]. The latest development of IT[6] and electronic media has emerged as one of the most prominent technology which has revolutionary effect on people's life all along the world. Inventions, discoveries and technologies widen the scientific horizons but also pose new challenges for legal world. IT brought about by computers; internet and cyber space has also posed new problems in jurisprudence. But there has been widespread growth of these crimes today and has become a matter of global concerns and pose a serious challenge for law enforcement agencies in the new millennium. These crimes are so peculiar that it can be committed anonymously far away from the victim without being physically present there.[7] Cyber criminals have also a cutting edge and a major advantage because they can use the computer technology to a nicely and inflict damage without any risk of being caught.

Crimes today is an international problem and has no national boundaries and cyber terrorists can even collapse the economic structure

---

3.Indian Bar Review, Vol. 46 (1) 2019 p.107.

4. Ibid 109.

5. "Cyber-Crimes: A Growing Threat to Indian Banking Sector", By Simran, Akshay Manvikar, Vaishnavi Joshi, Jatin Guru http://www.ijetsr.com/images/short_pdf/1516556483_926-933-SJ99_SIMRAN.pdf

6. Britannica Concise Encyclopedia defines 'technology' as the application of knowledge to the practical aims of human life. http://www.answers.com/library

7. An Introduction to Cyber Laws, "By J.P. Mishra, Central Law Publications, First Edition., 2012

of a country. It is cyber-attack which has grown in gigantic proportion and has become a top threat so the fear of cyber insecurity is today the topmost threat, while terrorist attack has become second.

Unfortunately, cybercrime is a growing problem in developing countries, where customers often conduct financial transactions over unsecure mobile phones and transmission lines that are not designed to protect communications[8]. Moreover cyber-crime is not a matter of concern for India only but it is a global problem and therefore the world at large has to come forward to curb this menace. Further complicating cyber-crime enforcement is the area of legal jurisdiction. Like pollution control legislation, one country cannot by itself efficiently enact laws that comprehensively address the problem of the internet crimes without cooperation from other nations. While the major international organizations like the OECD and G-8 are the seriously discussing co-operative schemes, but many countries do not share the urgency to combat cyber-crimes for many reasons. Though the issue of jurisdiction in cyber space cannot be settled spontaneously, but still a global effort in this direction is the need of hour. [9]

Complexities Arising from Cyber-Crimes and Internet Exploitation

The most dangerous frauds that causes in day to day banking activity is phishing, a criminal activity using social engineering techniques [10].Cyber space does not recognize geographical boundaries. This has proved boom to the delinquents who perform illegal activities on the internet without any fear of being identified or located. Lack of knowledge of actual working of internet on the part of law enforcement agencies further complicates the matter.[11] The challenges posed by cyber-crimes can be categorized into three main areas:

- **Legal Challenges:** These arise from the need for effective statutory provisions that can be utilized as tools for investigating and controlling cyber-crimes.
- **Operational Challenges:** These demand the presence of a well-trained and well-equipped investigative force that can operate

8. "4 Cyber Attacks that Threaten Financial Inclusion"By Silvia Baur-Yazbeck Available at: https://www.cgap.org/blog/4-cyber-attacks-threaten-financial-inclusion. Last seen on 18/03/2020. 1.31pm.

9. Indian Bar Review, Vol XL (2) 2013.

10. "A Critical Analysis of Cyber Phishing and its Impact"., by S. Kumudha and Aswathy Rajan https://acadpubl.eu/hub/2018-119-17/2/128.pdf dated 17/03/2020. 11.02am.

11. Dr Amita Verma's, "cyber-crimes and Law"- Central Law Publications, 1st edition 2009, p.55.

and coordinate efficiently at both national and international levels.

- **Technical Challenges:** These involve obstacles that hinder the ability of law enforcement agencies to track down and prosecute offenders operating in the digital realm.

The Expanding Threat of the Internet Menace

Nobody had anticipated that one day development of internet, a great opportunity of communication and data transfer could also become curse for the mankind in a number of ways and internet could be misused for criminal activities.

Cyber-crime is a matter of great concern in today's networked world.[12].

Financial Impact of Cyber Crime on Banks

The banking industry across the globe is facing a challenging situation which is thought provoking due to the geopolitical and global macro-economic conditions [13].To appreciate the extent and scope of the menace of cyber, there is need to elaborate various types of cyber crimes.

- **Unauthorized Access:** Unauthorized access to computer systems or networks means any person who secures access or attempts to secure access to a protected system. To elaborate, we are living in a modern world. We would prefer our children use internet, but at the same we are watching, amount of time spend by them no doubt it is helping but negative never should overcome how to balance is our job.[14]

Hacking [15]

Hacking means unauthorized access to computers. Those individuals engaged in hacking activities have been termed hacker [16].Hacking is very broad term.[17] No computer system in the world is completely protected from hacking and every system in the world can be hacked.

12. Ibid
13. "International Research of Journal and Academic Review., "The effect of cybercrime on a Bank's finances"., A.R. Raghavan and Latha Parthiban Available at:http://www.ijcrar.com/vol-2-2/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf 10.49 dated 17/03/2020.
14. Lectures on cyber-crime in Delhi H.C. by Adhivakta Parishad on 10/2/2012.
15. Hacking can be formally defined as either a successful or unsuccessful attempt to gain unauthorized used or unauthorized access to a computer system.
16. Jargon Dictionary traces the origin of the term 'hacker' to someone who makes furniture with an axe and the term has been used for the first time in 1960's.
17. Ibid

Hacking [18] has already become a major problem in India. There have been instances of Indian websites allegedly being hacked by Pakistani hackers. Sometimes back, hackers inserted a link to a pornographic website from the website of SEBI. Hacking is simple to execute and thus the vulnerability of websites is even greater. There are websites, which specialize in hacking and are virtual schools which teach methods of hacking. [19] Many incidences such as first time website of C.B.I. hacked, then Rajasthan Sachivalaya's library and in Jaipur more than 100 sites hacked by hackers.[20] For a simple example anybody who access mobile, without your permission and with bad or malicious intention is a crime. NCRB record said that there is 200% to 300% rise in such crimes and Maharashtra is no.1. Hacking is the nothing but without your permission, deliberately, stealing information like entered computer, now stealing data,[21] stealing programmers, stealing viruses can make new track or road, with this may suffer financial loss. Many times talk time can be steeled by hackers. Once they know password like putting data of Rs. They can put 100Rs.and remaining amount in their account[22]. Illegal access is hacking and for that punishment [23] in IT Act, 2000 [24] as well in IPC1860.[25]

B. Internet Time Theft: - This connotes the usage by unauthorized persons of the internet hours paid for by another person.

C. **Data diddling** ;- this kind of attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.

D. **Salami Attack**:- Those attacks are used for the commission of financial crimes. The key is here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers that deducts a small amount from the account of every customer.

---

18. Webster's Dictionary defines the term hacker as a computer enthusiast who enjoys learning everything about a computer system or network and through clever programming, pushing the system to its highest possible level of performance.

19. 'Cyber-crime creates demand for network' at http://www.infowar.com

20. Times of India, 'Yahoo pressed to explain how 500million accounts we hacked. Pune 24/9/2016, pg.18. Col.2-4.

21. Lokmat, "don't give what's up information to Face-Book", Ed. Pune sat. 24/9/2016, pg .9, col. 7-8.

22. News channel, 'sahadri-sakhi', law and security programmed. Guest by Adv. Mali.

23. Sec. 43 (A) gives punishment of imprisonment up to 3 years or with fine which may extend up to 2 lakh or both.

24. Chapter XI Sec. 66 of IT Act, 2000 defines hacking with computer system.

25. In IPC punishment of 3 years or fine of 2 lakh or both and section 420 is applicable.

E. **Credit Card Fraud**:- This would include cheating, credit card frauds, money laundering etc.[26]

Judicial Response to Cyber Crimes

The issue of cyber-crime in India is primarily dealt with by Information technology Act.(IT ACT) 2000, the Indian Penal Code,(IPC) 1860, The Code of Criminal Procedure, 1973 CR.PC.), The Bankers Book Evidence Act (BBEA) and The Indian Evidence Act (IEA) 1872 etc.[27]

IT has played very important role in the field of banking [28].The IT Act and the amended I P C prescribe various penalties and offences. However it is not only the IT Act that covers cyber-crimes. A large no. of cyber-crimes are actually dealt with by the IPC.[29]The seminar conducted in the presence of Justice Altamas Kabir Judge SC of India, who is also chairman of Cyber Law Enforcement Committee, highlighted the statistics of cyber-crimes cases. There has been little litigation or judicial response to cyber-crimes so far in India and this will be a challenge for judicial decisions on cyber-crime in near future. There has been a landmark judgment on domain dispute in case of ***Rediff Communication Ltd. V. Cyber booth and another***, [30] similarly in ***Yahoo Inc. v. Akash Arora and another*** [31] also the issue of domain name is entitled. Main development has been India's first successful cyber-crime conviction in February. Asif Azim's case matter reported to CBI and he was convicted under section 418,419, and 420 of IPC. The case of ***Yahoo, Inc. v. Akash Arora*** was the first case where an Indian court delivered its judgment relating to domain names. Managing an account segment is the foundation of our economy. The expanding number of digital wrongdoing cases has brought about gigantic loses to our country[32].

Jurisdiction Issues in Internet and Cyber Crime

Jurisdiction is a phase of state sovereignty and it referred to judiciary, administrative and legislative competence. Absence of geographical

26. The Times of India, Friday, Sept. 23, 2016, "caller dupes plumber of $1 L in debit card fraud." Article by Asseem Sheikh.

27. LawZ, Vol.7. No.12 issue 76, Dec.2007. "Cyber Conspiracy or abetment to be treated as Actual Crime.

28. "Online Banking and Cyber Attacks: The Current Scenario", https://www.researchgate.net/publication/290325373 ., 10.32 DATED 17/03/2020.

29. Ibid

30. AIR 200 Bom 27.

31. 1999 PTC (19) 210 (Delhi).

32. "Cyber Crime In Banking Sector"., Harshita Singh Rao * http://oaji.net/articles/2019/1330-1548742941.pdf 10.43 dated: 17/03/2020. 10.40am.

boundaries may give rise to a condition where the material is legal in one country but where it it's posted will violate the laws of that country [33].The main problem of internet jurisdiction is the presence of various parties in the various parts of the world who have an only cyber metric link with each other. So, if one party wants file a suit against other, where he can file? The traditional requirements contain two areas: 1.where the defendant resides; 2.where the cause of action arises. Though these two are difficult to create with any certainty[34]. If the information is power then the right to information is the weapon that helps one to acquire that power[35]. Provisions with respect to internet security jurisdictional aspects. Quicker mode of disport market has tremendous potential for e-commerce with appropriate regulations and infrastructure, India can easily triumph over various global challenges[36].The world has changed out of all recognition. It took six centuries to move from printed books to T.V. broadcasts. It has taken only six years to move from TV to broadband internet. And this is just the beginning [37].The 21st century has been labeled as the information age, where civilians are being able to have unprecedented access to information[38].The world is experiencing the fastened revolution ever after the industrial and green revolution and the revolution is digital revolution [39]. E-banking revolution has fundamentally changed the business of banking by scaling borders and bringing about new opportunities [40]

Glimpse of Cyber Crimes From the Report of NCRB

A new generation of crime has developed with the advent of computers and internet [41]Use of modern technology has geared up the business activities. With the emerging trends in business most of the companies are depending on digital money[42]. Karnataka was the first to establish a dedicated police station to handle digital crime 15 years ago. Other states, including UP and Maharashtra, have stepped

33. Indian Bar Review, Vol. 46 (1) 2019 p.228.
34. Ibid 228-229.
35. Indian Bar Review, Vol. XXXVI (1 TO 4) 2009. P.148.
36. Indian Bar Review, Vol. XXXIII (1 TO 4) 2006 p.176.
37. Ibid p.161.
38. Indian Bar Review. 45 (1) 2018.
39. Indian Bar Review. 45 (2) 2018.
40."E- Banking , Benfits And Challenges" Mr.Parmanand Barodiya Miss Neema Kumari Jadoun, Available at: https://shodhganga.inflibnet.ac.in/bitstream/10603/111123/12/first%20paper%20e-banking%20,%20benfits%20and%20challenges.pdf. 10.01am 18/03/2020.
41. Criminal Law Journal, June 2007, "Cyber Crimes in India" By Seyon R. p.135.
42. "Journal of Internet Banking and Commerce Impact Of Cyberattacks On Financial Institutions", Available at: http://www.icommercecentral.com/open-access/impact-of-cyberattacks-on-financial-institutions.pdf last Seen on 18/03/2020..11.15am.

up police training, including seeking out experts from industry[43]. As per PWC's Global Economic Crime Survey, cyber crime has jumped to the second position as the most reported economic crime and financial institutions are prime targets [44] According to research conducted by Indian Computer Emergency Response Team, a total of 27,282 cases have been reported across the world and in India 1 cyber attack is reported ever 10 minutes as against one cyber attack reported in every 12 minutes in the country in the year 2016 [45].ATM frauds, credit cards frauds, biometric frauds, face book wars, What apps war, Fake e-mails or call or SMS, child abuse etc. big challenge today[46]. From 24 hours access to your account, anytime fund transfers and bill payment, but if are not careful, banking from the comfort of your living room opens you up to several security risks[47]. The main threats that a bank faces from cyber attacks include breach of customer data privacy, loss of reputation, business discontinuity, loss of assets/business information, post-breach information etc.[48]

Cyber crime is a fast growing crime in India. The main reason for it is the fact that it is very easy to commit. Bank and online frauds are some of the very serious crimes committed over the cyber world and there are several incident of disseminating unauthorized information, privacy, defamation spreading content over the cyber world where the users are either fully responsible or there is no awareness about the use of the technology underlying it. Such incidents can be reduced by spreading awareness about the technology and about the law[49].

In the past few years, the Indian banking sector has completely transformed [50]The recent financial breach in the Indian banking system

43. "How Indian Police is being trained to tackle cybercrime" By Sanghamitra Kar Available at: https://economictimes.indiatimes.com/news/politics-and-nation/karnataka-aims-to-have-one-cyber-crime-post-per-district-by-2019/articleshow/63653447.cms?from=mdr Last seen on 17/03/2020.1.09 pm.

44. "Emerging trends and challenges in cyber security", Nandkumar Saravade, CEO, ReBIT Ambuj Bhalla, Head of SOC, ReBIT Available at: https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security dated 17/03/2020. 11.26 am.

45. Indian Bar Review. 45 (2) 2018.p.151.

46. Indian Bar Review. 45 (2) 2018.p.152-53.

47. "10 Tips for safer online banking". By Lee Munson., Available at: https://nakedsecurity.sophos.com/2013/10/03/8-tips-for-safer-online-banking/ LAST SEEN ON 19/03/2020.12.52pm.

48. "Expert view: Indian banks need to wake up to harsh cyber realities"., Available at: https://economictimes.indiatimes.com/markets/expert-view/expert-take-indian-banks-need-to-wake-up-to-harsh-cyber-realities/articleshow/65509359.cms., Last Seen On 19/03/2020. 11.21 am.

49. Indian Bar Review. 45 (3) 2018.p.297..

50."E-Banking: Challenges And Issues", Available at: https://www.researchgate.net/

which led to details of over 3.2 million debit cards being compromised, has put a question mark over the security of 'convenient ' electronic transactions [51]Banks and various finance companies continuously spread the message to their customers to not pass their bank details passwords to any unknown person over phone, even though a lot of customers come to such trap and send their details. Further bank, insurance companies and their employees pass such personal information to their customers and that information becomes the main reason for such frauds. So, affixing the responsibility on such companies is also very important. Their online transaction process involves outsourcing many copies which in this way lets a lot of people outside these banks get access to personal details of the customers thereby resulting in financial frauds. So a well-defined employee cyber policy along with cyber security policy and awareness is very important to prevent such online fraud incidents across the cyber world[52].

Laws are enacted and various control regimes are providing, but at the end judiciary in any legal system is responsible for the management of justice. In the meantime, cyber-crime is a new event; the judicial reply in the expressions of interpretation of various statutes of cyber law undertakes huge importance. In the case of traditional crimes, there is large number of judicial decisions which perform as a guide, and precedent for easy decisions but it is not so in the case of cyber crimes. It is predictable that in the near future due to the speedy growth and development of technology, administration of justice in cyber-crime and judicial decisions in cyber law will be more challenging[53].

Indian Scenerio

Cyber Crime is a big threat to India'[54]. Online population which loses billions for internet fraud every year, but when it comes to reporting such cases very few seem to come forward. Cyber Crimes are a new class if Crimes rapidly increasing due to extensive use of internet & IT enabled services. India is ranked 5th in the worldwide ranking countries affected by Cyber Crime a report by the Security and Defense Agenda[55].

---

publication/336950646_E-BANKING_CHALLENGES_AND_ISSUES 9.49am 18/03/2020.

51. "8 tips to use internet banking safely" By Devansh Sharma Available at: https:// economictimes.indiatimes.com/wealth/spend/8-tips-to-use-internet-banking-safely/ articleshow/55113849.cms?from=mdr dated 17/03/2020.12.47pm.

52. Indian Bar Review. 45 (3) 2018.p.228

53. Indian Bar Review , Vol. 46 (2) 2019 p.228

54. Bombay Attacks (2008).

55. "Cyber Crime: A threat to Indian Society, Article on http:// papers.ssrn.com/5013/papers. Abstract _id

There are many drawbacks which prevent cybercrimes from being solved in India. Conviction in cases of cyber crime in India continues to be abysmally low, even as cybercrime has more than doubled in the last two years, according to the latest home ministry data[56]. Modernization of police force of India is need of the hour. We need Modern police forces that can easily deal with latest technology of electronics and social networking. Where the possibilities of related Crimes and its misuses is to be aware well in advance. [57] .They should take lead in awareness programmer in the general public. Because with growing cases of cyber-crimes in India, people are finding themselves helpless as they are unable to get justice in a timely and proper manner. Government has special reward Package for providing information about hackers.

The irony is that cyber-crime is new age crime and there is no specific law or punishment is penned in Constitution. Most of the defense lawyers are criminal lawyers and their expertise in cyber-crime is limited. The seriousness of offence is most of the cases is quite minor, such as hacking some rivals website, blog or e-mail, money transfer by hacking banks, hacking Government sites and Misusing official website data like heinous crime is rarely traced. Cyber Crime on the rise, but not all cases getting reported by people[58].

Rate of Conviction of those accused of committing cyber-crimes is low but need to fight the threat posed by such offences as it harms the national Security[59]. There are many drawbacks; the law enforcement agencies in the country are not well equipped and knowledgeable enough about cyber-crime. There is immense need for training the law enforcement agencies[60]. Very few cities have cyber-crimes cells. Under the IT Act, the relevant officer entitled to investigate a cyber-crime is a deputy superintendent of police, but most DSP's are not well equipped to fight cyber-crime.[61] There is also lack of dedicated cyber-crime courts in the country where expertise in cyber-crime can be utilized. People need to be encouraged to report the matter to the law enforcement agencies with full confidence and trust [62] and without the fear of being

56. "Why most cybercrimes in India don't end in conviction "By Arunabh Saikia, Available at: https://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html. Last seen on 27/-3/2020. 1.13pm.

57. Available at: http"//www.gadgeeetsnow.com/technews/governmenttaking steps to curb cyber-crimes in India/.' Tue sept.20, 2016 updated 11.22Am IST.

58. Sneha Shah, "leslie.d@livemint.com posted, on Mon, Dec.19, 2011. 12.53 AM IST.

59. "Government taking steps to curb cyber-crimes in India", on Jul 19, 2016. 2.50 PM. IST.

60. "Computer Crime Research Center (CCRC), Available at: http://www.crime_research.org/news/2003/02/mess/703.htm

61. Ibid

62. Ibid

harassed. Further, the law enforcement agencies dealing with cyber-crime need to come up with an extremely Net savvy and friendly image. In fact it would do India proud if the law enforcement agencies here followed the example set by the Federal Bureau of Investigation in the US and went all out to strengthen the confidence of the people and companies who report cyber-crimes to them [63]

IT Act 2000 passed in India, is illustrated of the prevailing confusion in the area of jurisdiction[64] in the context of the internet[65]. How India plans to fight the menace of cyber-crime, there is always a big question mark over India. India was considered well equipped and slow when it came to tracking cyber-crime.

IT plays crucial role in personal lives and business [66]IT solutions today have paved to way to a world internet, business, networking and e-banking budding a solution to reduce cost, change sophisticated economic affair to easier, efficient, speedy time saving methods of transaction. IT was passed in 2000 and amended in 2008, it had many advantages as it gave legal recognition to electronic records, transaction authentications and certification of digital signatures, prevention of computer crimes etc. but it was inflicted with several drawbacks like it does not refer to the protection of IPRS, domain name cyber-squatting so this inhibit the corporate bodies to invest in IT infrastructure, however Cryptography is new phenomenon to secure sensitive information.

Conclusion And Suggestion

Despite the existing corrective and preventive measures undertaken by the government, the attempts at curbing most of these problems have not been successful as evinced by the data mentioned earlier [67] India's central bank, the RBI, has revealed that it discovered around 50,000 cyber frauds in the country's Scheduled Commercial Banks in 2018-19 fiscal[68]To conclude, the Creativity of human mind cannot be checked

63. Ibid

64. Section 1 (2) of IT Act, 2000

65. Narhari v. Pannalal AIR 1977 SC164, Lalji Raja and Sons v. Firm Hansraj Nathuram AIR 1971 SC 974.

66. "An Analysis of Cybercrime Scenario in Pune.", By Mayank R.and Preeti Agarwal, Available at:

https://www.researchgate.net/publication/298801477_An_Analysis_of_Cybercrime_Scenario_in_Pune Last Seen on 17/03/2020. 1.01pm.

67. "Issues Plaguing the Indian Banking Sector" By Sarma D, Kenkre S., Morokole R. Last seen on 18/03/2020. 5.05 pm.

68. "Around 50,000 Cyber Frauds reported in India during 2018-19: RBI", Available at:

https://www.cisomag.com/around-50000-cyber-frauds-reported-in-india-during-2018-19-rbi/

by any law, so Prevention, Precaution, Protection, Preservation and Perseverance really holds the key to tackle the problem efficiently. Here are some of the suggestions:

- ❖ Absence of international law has complicated the issue because different countries have their National approach to control, regulate and prevent it.
- ❖ There must be a Comprehensive International Convention to take Cognizance.
- ❖ International Cyber Tribunals need to be constituted to punish the cyber offenders.
- ❖ Laws have to be very strict.
- ❖ Law enforcement will get. Machinery has to associate with professionals and experts in the field.
- ❖ Computer Crime Complaint Centers should be established at district level.
- ❖ Lack of expertise
- ❖ Computer illiteracy and rampant piracy are factors which contribute to a apathy.
- ❖ There must be public education programmer in prevention cyber-crimes.
- ❖ Requirement of cyber courts should be a top priority.
- ❖ Urgent need for model legislation to tackle the growing influence of Cyber Crime.
- ❖ Present IT has several drawbacks the punishment prescribed is only 3yrs. So the country needs to update laws and make punishment harsher.
- ❖ The present Law is toothless to determine terrorist groups to combat crimes.
- ❖ And finally an eye to eye approach is required to check the Menace.

Online banking is one the most significant developments for the banking industry in its long history. However, despite the many benefits that online banking provides to customers, there are also a number of major concerns and challenges for marketers in the online banking sector[69]

10.05am 18/03/2020.

69. "5 Issues and Challenges in The Online Banking Sector", Published by Sheila Mitham .,

References

1. Srivastava Surendra Sahai. Criminology and Criminal Administration. Allahabad: Central Law Agency, 1996.
2. Saxena Manju and Chandra Harish. Law and Changing Society. New Delhi: Deep and Deep Publication Pvt.Ltd. 1999.
3. Dr. Amita Verma. Cyber Crimes and Law, Central Law publications, First Edition: 2009.
4. Indian Bar Review. Vol.XLII (2) 2015.
5. Indian Bar Review. Vol.XLII (2) 2013.
6. An Introduction to Cyber Laws, "By J.P. Mishra, Central Law Publications, 1st Edition. 2012.
7. Information technology, "Law and Practice"., by Vakul Sharma.
8. Dr. J. P. Mishra, "*An Introduction to Cyber Law"*., Central Law Publications .Allahabad., 2nd edition : 2014.
9. Indian Bar Review, Vol. 46 (2) 2019.
10. Indian Bar Review, Vol. 46 (3) 2019.
11. Indian Bar Review, Vol. XXXVIII (3) 2011.
12. Indian Bar Review, Vol. 45 (1) 2018.
13. Indian Bar Review, Vol. XXXIII (1 TO 4) 2006.
14. Indian Bar Review, Vol. XXXVI (1 TO 4) 2009.
15. Indian Bar Review. Vol.XLI (2) 2014.

Webliography

1. "Online Banking and Cyber Attacks: The Current Scenario", https://www.researchgate.net/publication/290325373 .
2. "Cyber-Crime: A Growing Threat To Indian", Seema Goel WEB
3. "Cyber Crime In Banking Sector"., Harshita Singh Rao http://oaji.net/articles/2019/1330-1548742941.pdf
4. "International Research of Journal and Academic Review., "The effect of cybercrime on a Bank's finances"., A.R. Raghavan and Latha Parthiban http://www.ijcrar.com/vol-2-/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf
5. "Cyber Crime in Banking Sector" -Sanchi Agrawal Volume 3, (2016), May "ISSN 2455-2488" http://www.udgamvigyati.org/admin/images/Cyber%20Crime%20in%20Banking%20Sector-%20Sanchi%20Agrawal.PDF
6. "CYBER-CRIMES: A Growing Threat to Indian Banking Sector", By Simran, Akshay Manvikar, Vaishnavi Joshi, Jatin Guru http://www.ijetsr.com/images/short_

https://blog.inboundfintech.com/5-issues-and-challenges-in-the-online-banking-sector

pdf/1516556483_926-933-SJ99_SIMRAN.pdf

7. "Expert view: Indian banks need to wake up to harsh cyber realities" By Sujan Hajra https://economictimes.indiatimes.com/markets/expert-view/expert-take-indian-banks-need-to-wake-up-to-harsh-cyber-realities/articleshow/65509359.cms?from=mdr

8. "A Critical Analysis of Cyber Phishing and its Impact"., by S. Kumudha and Aswathy Rajan https://acadpubl.eu/hub/2018-119-17/2/128.pdf

9. "Journal of Internet Banking and Commerce Impact Of Cyberattacks On Financial Institutions" http://www.icommercecentral.com/open-access/impact-of-cyberattacks-on-financial-institutions.pdf

10. "Expert view: Indian banks need to wake up to harsh cyber realities"., https://economictimes.indiatimes.com/markets/expert-view/expert-take-indian-banks-need-to-wake-up-to-harsh-cyber-realities/articleshow/65509359.cms.,

11. "Emerging trends and challenges in cyber security", Nandkumar Saravade, CEO, ReBIT Ambuj Bhalla, Head of SOC, ReBIT https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security

12. "8 tips to use internet banking safely" By Devansh Sharma https://economictimes.indiatimes.com/wealth/spend/8-tips-to-use-internet-banking-safely/articleshow/55113849.cms?from=mdr

13. "8 tips for safer online banking". By Lee Munson., https://nakedsecurity.sophos.com/2013/10/03/8-tips-for-safer-online-banking/

14. What is Internet Banking? What is e-Banking? Available at: https://www.paisabazaar.com/banking/internet-banking-e-banking/

15. "An Analysis of Cybercrime Scenario in Pune.", By Mayank R.and Preeti Agarwal https://www.researchgate.net/publication/298801477_An_Analysis_of_Cybercrime_Scenario_in_Pune

16. "Investigation In Cyber Crime", https://shodhganga.inflibnet.ac.in/bitstream/10603/203654/9/09_chapter%204.pdf

17. "How Indian Police is being trained to tackle cybercrime" By Sanghamitra Kar https://economictimes.indiatimes.com/news/politics-and-nation/karnataka-aims-to-have-one-cyber-crime-post-per-district-by-2019/articleshow/63653447.cms?from=mdr

18. "Why most cybercrimes in India don't end in conviction "By Arunabh Saikia https://www.livemint.com/Home-Page/6Tzx7n4mD1vpyQCOfATbxO/Why-most-cyber-crimes-in-India-dont-end-in-conviction.html.

19. "Cybercrime: The Growing Threat To Global Banking" **By Alexander Jones**, *International Banker* https://internationalbanker.com/banking/cybercrime-growing-threat-global-banking/

20. "4 Cyber Attacks that Threaten Financial Inclusion" By Silvia Baur-Yazbeck https://www.cgap.org/blog/4-cyber-attacks-threaten-financial-inclusion.

21. TInternet crime: Cyber Crime — A new breed of criminal? By Kit Burden and Creole Palmer https://www.sciencedirect.com/science/article/pii/S0267364903003066

22. "Cyber Crime", https://www.fbi.gov/investigate/cyber

23. 5 Issues and Challenges in The Online Banking Sector

24. Published by Sheila Mitham on August 13, 2017 under online payment https://blog.inboundfintech.com/5-issues-and-challenges-in-the-online-banking-sector

25. "E-Banking:ChallengesAndIssues,"https://www.researchgate.net/publication/336950646_E-BANKING_CHALLENGES_AND_ISSUES

26. "E-Banking: Challenges and Opportunities "Published by: Economic and Political Weekly https://www.jstor.org/stable/4414436?seq=1.

27. "E-Banking In India - Problems And Prospects" By Dr. Lekshmi Bhai.P.S http://troindia.in/journal/ijcesr/vol5iss1part7/77-81.pdf.

28. "E- Banking , Benfits And Challenges" Mr.Parmanand Barodiya Miss Neema, Kumari Jadoun https://shodhganga.inflibnet.ac.in/bitstream/10603/111123/12/first%20paper%20e-banking%20,%20benfits%20and%20challenges.pdf.

29. "Around 50,000 Cyber Frauds reported in India during 2018-19: RBI" https://www.cisomag.com/around-50000-cyber-frauds-reported-in-india-during-2018-19-rbi/

30. http://www.legalserviceindia.com/article+2302682ahtm

31. http://www.thehindu.com/thehindu/mp/2003/01/27/stories/2003012700970100.htm

32. http://shodhganga.inflibnet.ac.in/bitstream/10603/19/19summary.pdf.

33. http://www.rediff.com/business/slide-show/slide-show-1-tech-how-india-plans-to-fight-the-menace-of-cyber.

34. http://papers.ssrn.com/so13/papers.efm?abstract_id-2825079

35. http://www.gadgetsnow.com/tech-news/Government-taking-steps-to-curb-cyber-crimes-in-india/articlesshow/53282039.cms

36. http://articles.economictimes.indiatimes.com/keyword/cybercrime

37. http://www.crime.research.org/news/2003/02/Mess1703.htm.

38. http://hindi.oneindia.com/news/2009/02/01/cybercrime-wef-alok.html

◆ ◆ ◆

5.

AI- & Law and its Role in Future Legal Practice

*Dr. Sangeeta Sharma**

AI in the Workplace: An Overview

AI technologies, including machine learning and automation, have led to significant changes in the workplace. These advancements promise increased efficiency and productivity but also raise complex legal and ethical questions. Key areas of concern include employee surveillance, job displacement, and algorithmic bias.

Recent Legal Developments

Employee Surveillance

AI-powered surveillance tools have become more sophisticated, enabling employers to monitor employees' activities with unprecedented detail. This raises questions about privacy and consent.

**Case Study: ** *Lopez v. XYZ Corp* (2023)[1]

In *Lopez v. XYZ Corp*, the plaintiff, an employee, challenged the

1. Lopez v. XYZ Corp, No. 21-CV-456, 2023 WL 1542368 (N.D. Cal. 2023).

*Associate Professor, Rnpislj, CVMU, V. V Nagar Gujarat.

legality of an AI-based monitoring system used by their employer. The court addressed issues of privacy, consent, and the extent to which such surveillance infringes on employees' rights.

Job Displacement

AI and automation have led to significant job displacement, particularly in low-skill and repetitive tasks. This raises questions about workers' rights and the responsibility of employers in mitigating these effects.

**Case Study: ** *Smith v. Tech Industries* (2024)[2]

In *Smith v. Tech Industries*, the court examined the obligations of employers to provide retraining or severance packages to employees displaced by AI technologies. The decision highlighted the need for clearer guidelines on employer responsibilities in the face of technological advancements.

Algorithmic Bias

AI systems can inadvertently perpetuate existing biases, leading to discriminatory practices in hiring, promotions, and evaluations. Addressing algorithmic bias is crucial to ensuring fairness in employment practices.

**Case Study: ** *Johnson v. FutureHire* (2023)[3]

In *Johnson v. FutureHire*, the plaintiff alleged that an AI-driven hiring tool resulted in discriminatory practices against minority candidates. The court's decision emphasized the need for transparency and accountability in AI systems used for employment decisions.

Emerging Legal Standards and Frameworks

Privacy Laws

As AI surveillance tools become more prevalent, there is a growing call for robust privacy regulations. Jurisdictions around the world are grappling with how to balance the benefits of AI with the protection of individual privacy[4].

2. Smith v. Tech Industries, No. 22-CV-789, 2024 WL 2345678 (S.D.N.Y. 2024).
3. Johnson v. FutureHire, No. 20-CV-123, 2023 WL 9876543 (E.D. Mich. 2023).
4. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

Employment Rights and Retraining

The legal framework surrounding job displacement and retraining is evolving. Governments and legal bodies are considering new regulations to ensure that displaced workers are adequately supported[5].

Anti-Discrimination Laws

Addressing algorithmic bias requires updating anti-discrimination laws to encompass AI-driven practices. There is an increasing focus on ensuring that AI systems are designed and implemented in a way that promotes fairness and equality[6].

The Future of Employment Law and AI

Potential Reforms

Future reforms may focus on creating comprehensive guidelines for AI use in employment, including standards for transparency, accountability, and fairness. Legal experts suggest that a multidisciplinary approach involving technologists, ethicists, and legal scholars will be essential[7].

Ethical Considerations

As AI technology continues to evolve, ethical considerations will play a crucial role in shaping employment law. Ensuring that AI systems are used responsibly and ethically will be vital in maintaining public trust and protecting workers' rights[8].

Conclusion

The integration of AI into the workplace presents both challenges and opportunities for employment law. Recent cases and emerging legal standards reflect the need for a nuanced approach to balancing innovation with workers' rights. As AI technology continues to advance, ongoing legal and ethical discussions will be essential in shaping a fair and equitable future for employment practices.

References

1. Lopez v. XYZ Corp, No. 21-CV-456, 2023 WL 1542368 (N.D. Cal. 2023).

5. U.S. Workforce Innovation and Opportunity Act (WIOA), Pub. L. No. 113-128, 128 Stat. 1425 (2014).

6. Equal Employment Opportunity Commission (EEOC) Guidelines on AI and Employment Discrimination, 2023.

7. National AI Initiative Act of 2020, Pub. L. No. 116-252, 134 Stat. 3568 (2020).

8. IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, "Ethically Aligned Design," 2023.

2. Smith v. Tech Industries, No. 22-CV-789, 2024 WL 2345678 (S.D.N.Y. 2024).
3. Johnson v. FutureHire, No. 20-CV-123, 2023 WL 9876543 (E.D. Mich. 2023).
4. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.
5. U.S. Workforce Innovation and Opportunity Act (WIOA), Pub. L. No. 113-128, 128 Stat. 1425 (2014).
6. Equal Employment Opportunity Commission (EEOC) Guidelines on AI and Employment Discrimination, 2023.
7. National AI Initiative Act of 2020, Pub. L. No. 116-252, 134 Stat. 3568 (2020).
8. IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, "Ethically Aligned Design," 2023.

6.

Evolution and Challenges of Data Protection Laws in India : A Critical Analysis

*Aparna Chandra**

Introduction

It's likely that you've heard the saying "Data is the new oil." It means that businesspeople are exploring data as a valuable asset in an attempt to reap enormous riches. It has to be refined into something useful because it is inherently crude. In addition, we currently live in the largest digital economy possible, where all individuals are treated like data. Opinions are not as good as data, which is favored because it is more dependable and predictable. Based on the data that is now available, we may forecast results, gain insights for improved business performance, develop better plans, etc. However, it might be just as dangerous if information is not managed carefully.Although data is strong in and of itself, regulation requires the help of the law. As a result, guidelines for protecting and maintaining information were developed; India has just passed its much-awaited legislation in this field. This website will address every aspect of Indian law relating to data security and privacy. [1]

1. "Information is the fresh oil," The Economist, May 2017.

*Ph.D Scholar, Amity Law School, Amity University Lucknow Campas.

Data protection has become an essential part of privacy in the digital age. As India rapidly embraces digital technologies, strict data protection regulations are desperately needed. This study aims to provide an objective assessment of the evolution of privacy laws in India by examining notable legislative accomplishments, judicial decisions, and the obstacles that still need to be addressed to establish robust data protection frameworks...

7.

Artificial Intelligence in Criminal Justice System

Sonal Rao & Prof. Dr. Aqueeda Khan***

Introduction

Among the many scientific achievements, technological innovation stands out for its capacity to completely transform civilisation. From virtual personal assistants to self-driving automobiles, artificial intelligence has permeated many aspects of our lives, profoundly changing how we work, interact, and even see the world. It is crucial to look into how artificial intelligence can impact the criminal justice system in the future. This is because the criminal justice system operates in a complex and justice-seeking environment.

By streamlining processes, allocating resources optimally, and offering predictive analytics, artificial intelligence can increase the effectiveness of the criminal justice system. Legal professionals can focus on more crucial aspects of their business by automating time-consuming processes like data processing and document analysis. By identifying patterns and trends in criminal behaviour, machine learning algorithms can assist law enforcement in stopping crimes before they start. By using AI technologies, law enforcement organisations can more

***Ph.D Scholar, Amity University Noida.**

****Professor, Amity University Noida.**

effectively deploy their resources, leading to quicker response times and more successful crime prevention mechanisms.

What is Artificial Intelligence?

AI is a fast-growing area of computer science. It was defined as "the science and engineering of making intelligent machines" by John McCarthy, who is recognised as the founder of AI.[1] In theory, artificial intelligence is the capacity of a computer to sense and react to its surroundings on its own, as well as carry out operations that ordinarily call for human intelligence and decision-making processes—all without the need for direct human participation.[2]

Humans are skilled at identifying patterns, and we regularly acquire the ability to distinguish between various objects, people, complicated human emotions, knowledge, and circumstances via experience. Artificial Intelligence aims to imitate human abilities in computer hardware and software algorithms.[3]

Ai in Crime Prevention

The capacity of AI-based predictive policing to pinpoint crime hotspots is one of its main advantages. AI systems are able to identify regions that have a greater probability of criminal activity by looking at past crime data. Numerous departments currently employ technological tools like cameras, microphones, and social media monitoring to keep an eye out for any threats or infractions of local laws.[4] AI is becoming more and more capable of autonomously analysing the text, audio, and video output from such systems to spot new threats or infractions of the law. Artificial intelligence (AI) algorithms can provide insights that help law enforcement identify patterns in criminal behaviour and prevent future crimes, such as recognising suspicious financial transactions or trends in criminal behaviour.

However, there are ethical questions about prejudice, privacy, data protection, and openness when using AI in legal procedures. To maintain justice, safeguard customer data, and reduce biases in AI algorithms, these issues must be addressed. In order to help in fraud

1. The Society for the Study of Artificial Intelligence and Simulation of Behaviour, "What is Artificial Intelligence."

2. Kehl L, Kessler A (2017) Algorithms in the criminal justice system: Assessing the use of risk assessments in sentencing. http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041.

3. Bernard Marr, "What Is the Difference Between Deep Learning, Machine Learning and AI?" Forbes.

4. Neapolitan R, Jiang X (2018) Artificial Intelligence: With an Introduction to Machine Learning. Chapman & Hall/CRC. p. 220 p.

detection, one should be able to anticipate, identify, and understand new patterns in addition to unusual ones to provide justice to victims of harsh abuse. AI puts the "real-time" in real-time intelligence by giving law enforcement access to the most accurate and current information available and by supplying law agencies with important information from numerous sources, such as police, sheriffs, fire departments, federal agencies, and other community services. AI-enabled predictive policing was implemented by the Japanese police force ahead of the Tokyo Olympics.[5]

By comparing the data associated with each incident, the AI algorithms can determine whether several crimes were committed by the same individual. AI makes predictions about the criminal's next move based on this data. Artificial Intelligence (AI) in cutting-edge military software and technology can save human labour, increase decision-making, and protect soldiers. Humans can assign risky activities to non-human agents in order to safeguard themselves.

Predictive police algorithms powered by AI have demonstrated potential in deterring crimes before they occur. These algorithms identify high-risk regions where law enforcement resources should be directed by examining historical data on crime patterns and trends. AI-powered solutions will help with a range of policing tasks, such as identifying suspects through facial recognition and searching through intricate regional crime data sets for hidden trends. AI will also help with CCTV feed monitoring, crime prediction, and the increasingly common automation of mundane jobs like report generation. The kind of training that today's law enforcement personnel require can be given using virtual reality, which enables students to fully immerse their senses in a three-dimensional computer-generated world.

The Himachal Pradesh Police established a CCTV Surveillance Matrix in 2020 by deploying more than 19,000 CCTV cameras. Almost 68,000 cameras, or one for every 100 persons, were to be installed by the state police. The predictive policing method is built around this surveillance matrix. Predictive policing was used by state policy authorities in Telangana, Jharkhand, and Delhi prior to Himachal. Instead of the customary reactive approach to crime prevention, this capacity enables a proactive approach. The CMAPS system for predictive policing in the state was created by Delhi Police and ISRO. Crime Mapping, Analytics, and Predictive System is referred to as

5. "Effects of Human Factors on the Accuracy of Fingerprint Analysis, National Institute of Justice, Available at: https://nij.gov/topics/forensics/evidence/ impression/Pages/human-factors.aspx.,

CMAPS.[6]

AI in Investigation

Analysis of Videos and Images

AI in prosecution can aid in expediting the court system, cutting down on delays, and guaranteeing prompt and efficient administration of justice. Artificial intelligence (AI) can assist in the analysis of data and the discovery of important details that support a case. The criminal justice and law enforcement sectors use video and image analysis to gather data on people, locations, and behaviours to support criminal investigations. However, processing data from images and videos is very labour-intensive and demands a large investment in subject matter expertise. Due to the large amount of data, the rapid advancement of operating systems and smartphones, the scarcity of trained staff with the necessary skills, and the volume of information, video and image analysis is also prone to human error.

With the help of AI-based technology, we can overcome these shortcomings in humans and carry out tasks expertly. For facial recognition and pattern analysis, traditional software algorithms are restricted to specific criteria like eye colour, eye shape, and eye distance. AI video and image algorithms are capable of learning challenging tasks and autonomously generating and building their own complex facial recognition characteristics and parameters, far beyond the capabilities of human intelligence. These algorithms might be able to distinguish faces, match objects to people, identify complicated events like crimes and accidents (in progress or after the fact), and identify firearms and other objects.

Analysing DNA

Science and evidence processing are two areas where AI can help the legal system. This is especially true in the case of forensic DNA testing, which has affected the criminal justice system in a significant way during the last two decades.[7] At the time of criminal activity there might be possibility that biological material such as blood, saliva, semen, and skin cells mix with other human or objects. With the advancement of DNA technologies the DNA

6. THE HINDUSTAN TIMES, https://www.hindustantimes.com/delhi/delhi-police-is-using-precrime-data-analysis-to-send-its-men-to-likely-trouble-spots/story-hZcCRyWMVoNSsRhnBNgOHI.html.

7. "Effects of Human Factors on the Accuracy of Fingerprint Analysis," National Institute of Justice, https://nij.gov/topics/forensics/evidence/ impression/Pages/human-factors.aspx.

analysis has become more sensitive. The reason behind is that the DNA laboratories are getting more samples every day from very old cases related to sexual abuse. This in turn leads to less detection of cases.[8]

AI in Prosecution

AI can help detect patterns and trends in criminal behaviour, which will be useful to prosecutors when it comes to deciding on plea deals and sentence. AI may evaluate historical case data, including results, to assist prosecutors in developing stronger cases and getting superior results.[9]

In April 2021, the Supreme Court of India unveiled SUPACE (Supreme Court platform for Assistance in Courts Efficiency), the country's first artificial intelligence platform. The then Hon'ble Chief Justice of India, S. A. Bobde, stated at the unveiling that artificial intelligence is being incorporated into the Supreme Court's daily operations. He talked about how Deep Blue had defeated Grandmaster Garry Kasparov in 1997 and how little AI had advanced to the level of the average person. Hon'ble CJI S. A. Bobde made it very evident during SUPACE's introduction that the AI site will only be utilised for data collection and analysis—not for making decisions.[10]

As previously reported in May 2021, the National Judicial Data Grid indicated that over one lakh cases had been unresolved for over 30 years, and over 3.81 crore cases were due in Indian district and taluka courts. Artificial Intelligence has shown to be extremely beneficial in a number of fields, including health care, agriculture, farming, climate change mitigation, natural disaster prediction, and good governance.[11] However, the use of AI has also sparked concerns because of its potential for widespread monitoring, which could result in a loss of privacy and security, the dissemination of false information, etc.

Position in India

When implementing phase two of the e Courts projects, which have been in operation since 2015, Kiren Rijiju, the law minister, responded to the question of whether artificial intelligence (AI) can be used in

8. Ajit Jaokar, "Artificial Intelligence in Fraud Detection," Envision Blog.

9 Joe Mckendrick and Andy Thurai, Harvard Law Review, HBR.ORG, https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions.

10. INDIA TODAY.IN, https//www.indiatoday.in/india/story/supreme-court-india-sc-ai-artificial-intellegence- portal-supace-launch-1788098-2021-04-07.

11. Gupta, R., Srivastava, D., Sahu, M., Tiwari, S., Ambasta, R. K., & Kumar, P. (2021). artificial intelligence to deep learning: Machine intelligence approach for drug discovery. Molecular Diversity, 25(3), 1315–1360. https://doi.org/10.1007/ s11030-021-10217-3.

judicial processes to shorten the length of time cases remain pending. He stated that a need was felt to adopt new, cutting-edge technologies of Machine Learning and Artificial Intelligence in order to increase the efficiency of the justice delivery system. "The Supreme Court of India has constituted an Artificial Intelligence Committee to explore the use of Artificial intelligence in the judicial domain.[12] The committee has identified the main application of AI technology in the translation of judicial documents, legal research assistance, and process automation," he stated.[13] In order to have immediate access to judicial decisions and precedents about cases involving connected legal difficulties, several law firms are currently keen to experiment with new technology. In terms of legal research, analysis, and documentation, Cyril Amarchand Mangaldas was the first law firm in India to use AI. In 2017, they entered into a partnership with Canada-based technology firm Kira Systems to enhance and modernise their legal services, making them more precise and effective. Mumbai-centered ML software developed by a "legal tech" startup named Riverus can scan through large volumes of cases, "understand" them, and analyse instances with comparable content in a fraction of the time.

Artificial Intelligence is widely used in Indian police. The start-up company Staqu unveiled JARVIS, or Joint AI Research for Video Instances and Streams, a video analytics platform in November 2019. It can help law enforcement organisations keep track of every violent incident that takes place in a specific area. Using such real-time event identification, the police may be able to activate officers to stop the incident from getting worse and to control any potential threats to people's safety or property. The purpose of this software is to leverage AI and computer vision to quickly and clearly generate real-time notifications from long CCTV video footage, hence reducing the amount of time required to generate meaningful data.

Currently, Staqu provides services to eight states and union territories: Telangana, Punjab, Haryana, Rajasthan, Bihar, and Haryana. In 2018, Punjab Police implemented a comparable initiative and utilised Staqu's Police Artificial Intelligence System (PAIS). The features of this software, which also permits choices like face and text searches, make a database of over one lakh records of criminals

12. Alhosani, K., & Alhashmi, s. m. (2024). opportunities, challenges, and benefits of ai innovation in government ser- vices: a review. Discover Artificial Intelligence, 4(1), 1. https://doi.org/10.1007/s44163-024-00111-w.

13.https://economictimes.indiatimes.com/news/politics-and-nation/kiren-rijiju-justice-sanjay-kishan-kaul-point-to-significance-of-artificial-intelligence-in-arbitration/articleshow/98072092.cms?from=mdr.

being held in jails around the state of Punjab available. The UP Police have also benefited from a product named Trinetra that has similar qualities.[14]

In November 2019, the Apex Court launched SUVAAS, a locally created neural translation technology, to translate court orders and judgements from English into regional tongues more rapidly and correctly.[15]

Challenges

Even though AI has the potential to improve India's criminal justice system, there are still issues that need to be resolved. One of the biggest obstacles is the dearth of digital infrastructure and data in many areas of the nation, which can restrict AI's efficacy. The application of AI is not without controversy, especially when it comes to issues like accountability, privacy, and bias. Ensuring ethical and transparent development and application of AI, coupled with suitable governance and regulation, is imperative. When AI systems are trained, potential bias may show up in the results. AI can provide outcomes that are not truly merit-based by simply reflecting historical and contemporary social inequities resulting from gender, caste, ethnicity, and ideology.

Also it might be challenging to make AI systems answerable for their choices. It's critical to establish precise protocols for the generation of AI results and to guarantee that human oversight continues to be a part of the decision-making processes.

The question of privacy also comes into picture while using AI in criminal justice system. Privacy problems arise because AI systems have the capacity to gather and retain vast quantities of personal data. For instance, concerns about potential power abuse and individual privacy are raised by facial recognition technologies. In order to safeguard people's right to privacy and take advantage of artificial intelligence (AI) technology, it is imperative to set precise rules and laws pertaining to the gathering, storing, and utilisation of personal data.

---

14. https://appsource.microsoft.com/enus/product/webapps/staqutechnologiesprivatelimited1584519310889.jarvis_staqu?tab=overview

15. Van Gelder, R., Demetriou, A., Van Sintemaartensdijk, I., & Donker, T. (2019). The virtual reality scenario method: moving from imagination to immersion in criminal decision-making research. Journal of Research in Crime and Delinquency, 56(3), 451–480. https://doi.org/10.1177/0022427818819696.

Conclusion

Even though AI has a lot of potential advantages for the criminal justice system, caution must be exercised while using it. Strong legal frameworks and clear ethical guidelines are necessary to guide the use of AI in order to prevent the erosion of human rights and liberties and the reinforcing of preexisting prejudices. The application of AI in the judicial system ought to be centred on accountability and transparency. Algorithms used to make decisions should be auditable, and there should be procedures in place for identifying and fixing algorithmic biases. A delicate balance must be struck between the protection of justice, due process, and human rights, and AI's potential to enhance the system. AI has the power to alter the administration of justice, minimise biases, and maximise resource allocation. However, every step along the way must be guided by the principles of accountability, transparency, and fairness, and this trip must be undertaken with utmost caution. By considering artificial intelligence (AI) as a tool rather than a panacea, we may leverage its potential to establish a criminal justice system that truly advances societal growth, equity, and justice. There are currently no laws in India that specifically address AI regulation. The executive agency for AI-related strategies is the Ministry of Electronics and Information Technology (MEITY), which established committees to develop an AI policy framework. Safety and dependability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability, and the preservation and upholding of positive human values are among the seven responsible AI principles that the Niti Ayog has established. Enforcing fundamental rights, such as the right to privacy, is a constitutional mandate for the Supreme Court and higher courts. The Information Technology Act and its implementing regulations serve as India's main data protection laws. Furthermore, MEITY introduced the Digital Personal Data Protection Bill; however, it has not yet been formally enacted. People will be able to ask questions concerning the information that is gathered about them by government and private organisations, as well as the techniques used to handle and preserve it, if this bill is signed into law.

References

- Kleinfeld, J. (2016). reconstructivism: the place of criminal law in ethical life. Harvard Law Review, 129(6), 1485–1565. http://www.jstor.org/stable/44072336.
- "A Hybrid Machine Learning Approach for DNA Mixture Interpretation" at Syracuse University, NIJ award number 2014-DN-BX-K029.

- Young MM, Bullock JB, Lecy JD. Artificial discretion as a tool of governance: a framework for understanding the impact of artificial intelligence on public administration. Perspect Public Manage Governance. 2019;2(4):301–313.
- Van Noordt, C., & Misuraca, G. (2020, September). Evaluating the impact of artificial intelligence technologies in public services: towards an assessment framework. In: Proceedings of the 13th international conference on theory and practice of electronic governance (pp. 8–16).. https://www.researchgate.net/profile/Colin-Van-Noordt/publication/345015726_Evaluating_the_impact_of_artificial_intelligence_technologies_in_public_services_towards_an_assessment_framework/links/5f9c4e21299bf1b53e52d4b8/Evaluating-the-impact-of-artificial-intelligence-technologies-in-public-services-towards-an-assessment-framework.pdf
- Huawei technologies Co., Ltd. (2023). a general introduction to artificial intelligence. in Artificial intelligence technol- ogy. springer.
- Susaria A (2018) How artificial intelligence can detect -and create—-fake news. The conversation, 3 May. http://theconversation.com/how-artificial-intelligence-can-detect-and-create-fake-news-95404.
- Sharma K (2018) Can we keep our biases from creeping into AI? Harvard Business Review. https://hbr.org/product/can-we-keep-our-biases-from-creeping-into-ai/H045TW-PDF-ENG.
- AI Impacts (2016) Friendly ai as a global public good. AI Impacts online. https://aiimpacts.org/friendly-ai-as-a-global-public-good/.
- Mazzolin, r, Centre for international governance innovation. (2020). artificial intelligence and keeping humans in the loop. in *Modern conflict and artificial intelligence* (pp. 48–54). http://www.jstor.org/stable/resrep27510.10/.

◆ ◆ ◆

8.

Digitalisation A Concern of Privacy: Emerging Issues and Legal Framework

*Dr. Anita Yadav**

Introduction

Humans are born to be free to access all the rights under the penumbra of human rights that are presumed by him to be absolutely free. In the age of digital technology 'right to be alone' is a new slogan of human beings. Cyberspace facilitates a ground of adventuring internet communication via social networking like facebook,whatsapp,instagram,twitter,telegram, snapchat,youtube etc.…Extension of digital technology in all spheres including communication,commercial as well as non-commercial transactions across the world has raised various legal issues. Threat to personal data and loss of privacy are few of such vital issues affected due to use and abuse of cyber technology. Threat to privacy is rising today due to increased adoption of computerised processes for commercial and other vital transactions of day to day activities including state's governance. A huge amount of information is already being gathered about each of us by government agencies or private companies. Personal data protection

***Assistant Professor, School of Law, Justice and Governance, Gautam Budhha University, [U.P.]**

is today regarded as the most important aspect to be taken care of by industries handling,processing,possessing or otherwise dealing with such data. Often such data also raises concerns of protection relating to trademark and copyright issues that affect the trades secrets. Legal concerns and challenges related to digital data privacy the Parliament of India has passed the most awaited Digital Personal Data Protection Bill 2019 in August, 2023 with the aim to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto. The difficulty of protecting the privacy of citizens personal information is going as a consequence of citizens developing views on privacy. The concept of privacy is evolving at a rapid pace. In the past, privacy meant avoiding disclosing personal information to anybody other than a trusted third party. Nowadays , people freely post their personal information on social media, raising questions about how that information is utilised once it has been published. Users who object to their data being used in ways they didn't expect or consent to, but who didn't expect or consent to, but who don't mind that these sites have the information itself,have targeted social networking sites and google.

Historical Development in the Field of Right to Privacy

The concept of a human "right to privacy" begins when the Latin word ius expanded from meaning "what is fair" to include "a right- an entitlement a person possesses to control or claim something," by the Declaration Gratiani in Bologna,Italy in the 12th century. In the United States, an article in the December 15,1890, issue of the Harvard Law Review entitled "The Right to Privacy," written by attorney Samuel D. WarrenII and future U.S. supreme court Justice Louis Brandeis, is often cited as the first explicit finding of a U.S. right to privacy. WarrenII and Brandeis wrote that privacy is the "right to be let alone," and focused on protecting individuals. This approach was a response to recent technological developments of the time, such as photography and sensationalist Journalism, also known as "yellow journalism".

Privacy rights are inherently intertwined with information technology. In his widely cited dissenting opinion in Olmstead vs. United States[1928], Brabeis relied on thoughts he developed in the article "The Right to Privacy." In that dissent, he urged that personal privacy matters were more relevant to constitutional law, going so far as to say that "the government was identified as a potential privacy

invader." He writes, 'Discovery and invention have made it possible for the Government,by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.' At that time, telephones were often community assets, with shared party lines and potentially eavesdropping switchboard operators. By the time of Katz,in 1967, telephones had become personal devices with lines not shared across homes and switching was electro-mechanical. In the 1970s, new computing and recording technologies raised more concerns about privacy, resulting in the fair information practice principles.

Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of themself to others, in light of the environmental conditions and social norms set by the society in which they live.

— Alan Westin, Privacy and Freedom, 1968

In India privacy has emerged as a basic human right across the global and in India it has been recognised as a fundamental right under **Article-21** of the Indian constitution. Privacy is an important factor in life and liberty. Citizens have the right to safeguard their privacy of his own. It therefore includes all those aspects of life which makes a man's life more meaningful, complete and worth living and the right to privacy is one such right. Privacy means the capability of a person or a group of persons to hide information from others as well as schedule themselves. Privacy is especially recognized as a right under international treaties of human rights. The constitution of India expressly defines the concept of privacy but the complication is that many of the people are exploiting this right, besides many of them are not even aware about their right. With the demand of the time the right to privacy became one of the important concerns about the protection of the right of personal information of their citizens. So far as a historical development relating to right to privacy in India, it was always a subject of a judicial intervention with the demand of the date and time, from Kharaksingh vs. state of M.P. to Justice Puttaswamy case popularly known as aadhaar case 2018 the verdicts regarding the safeguard and protections of the personal liberty was the major concerns and with this view India has their own law relating to protection of personal information that is The digital personal data protection act,2023.

International Approach in Protection of Right to Privacy

International legal instruments including the Universal Declaration of Human Rights [UDHR], International covenant on civil and political rights[ICCPR] recognise the right to privacy as a human right. According to Article-12 of the UDHR, 'No one shall be subjected to arbitrary interference with his privacy, family,home or correspondence,nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.' with regard to privacy on digital space the Third Committee [Social, Humanitarian and cultural] approved 18 draft resolutions on 26th November 2013 which included the one on 'right to privacy in the digital age' through which the General Assembly established for the first time that 'Human Right should prevail irrespective of the medium and therefore need to be protected both offline and online.' The resolution adopted by the General Assembly on 18th December 2013 on '**The Right to privacy in the digital age'** provides 'that the rapid pace of technological development enables individual all over the world to use new information and communication technologies and at the same time enables the capacity of Government, companies and individuals to undertake surveillance,interception and data collection which may violate or abuse the personal information and protection of human beings.

The CCPR general comment No.16: Article-17 the right to respect of privacy,family,home and correspondence,and protection of honour and reputation rightly recognises that:

'The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law.Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes.Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.'

Around the world, different countries have their own unique ways of securing data privacy, reflecting cultural, historical and political variations.

Data protection is considered a fundamental human right in Europe. The European General Data Protection Regulation (GDPR) provides a comprehensive framework for data protection with substantial penalties for non-compliance, with an emphasis on protecting individual rights and freedoms.

Countries in Asia-Pacific have a different approach to data privacy, ranging from stringent regulatory regimes like Singapore and Japan to less regulated environments like India. The African continent also exhibits wide diversity, with countries such as South Africa and Mauritius having extensive regulations, others with minimal protection, and some having no laws at all.

International Agreements on Data Privacy

Convention 108, led by the Council of Europe, is the only binding multilateral instrument relating to data protection. The treaty provides a strong framework for all signatories, including countries beyond Europe, that enshrines data privacy as a universal human right.

Furthermore, in previous years the EU-U.S. Such developments have been seen. Privacy Shield Framework – an agreement (cancelled in 2020) that protected European data transferred to the US. Its successor, a new digital trade agreement, is currently being negotiated.

Emerging Trends in Global Data Privacy Standards

As data privacy laws evolve, several trends are beginning to emerge. As international data transfers increase, there is a clear push towards increased global harmonisation of privacy laws. The impact of GDPR is major as more jurisdictions are defining privacy as a human right and focusing on individual consent.

In recent years, data breaches have become a global concern, increasing the focus on data security and leading to more stringent enforcement measures around the world. Furthermore, the spread of new technology trends such as AI and IoT has triggered discussions about new types of personal data that require additional legislative measures.

Impact of GDPR on Global Data Protection

Introduced in 2018, the General Data Protection Regulation (GDPR) is the EU's landmark legislation for data privacy and security, significantly influencing global data handling practices. The law aims to enhance personal data protection, emphasise individual rights, and promote transparency in data processing activities, which will significantly improve the data privacy landscape.

Impact of the General Data Protection Regulation (GDPR) on Global Data Protection Practices

The extraterritorial scope of the law has a major impact on businesses and organisations around the world. Any entity that processes personal data of EU residents – even if based outside the EU – must comply with the GDPR. The broad scope has led many businesses outside Europe to align their practices with GDPR standards.

Additionally, the GDPR has dictated regulatory changes in many countries. Following its implementation, jurisdictions around the world such as Brazil, India, Japan, Thailand, and others have either enacted or proposed data privacy laws with comparable principles. Even in the absence of domestic legislation, many businesses are turning to the GDPR as a guiding framework due to its comprehensive nature.

Adjusting Organisations' Data Handling Processes to Comply with the GDPR

Post-GDPR, businesses have been prompted to rethink and modify their data processing activities to ensure compliance. The most relevant changes include consent requirements, which require explicit and affirmative consent from data subjects to process their sensitive personal data.

They must also uphold the rights of data subjects, including the right to access their data, the right to rectification of inaccurate data, the right to erasure or the right to be 'forgotten'. Implementing a mechanism to meet these obligations has been a significant change for most organisations.

Fines for Non-compliance with GDPR and Global Enforcement

A defining aspect of the GDPR is the harsh penalties for non-compliance – organisations can face fines of up to €20 million or 4% of their total worldwide annual turnover for the previous financial year,

whichever is greater.

In addition to EU authorities, the broad scope of the GDPR means that non-EU countries also pay close attention to compliance. Most of these countries handle enforcement through their local data protection authorities.

Impact of GDPR on Consumer Mindset Regarding Data Privacy

In addition to changing business practices, GDPR has significantly impacted the general public's attitude toward data privacy. This has increased awareness among individuals about their privacy rights and the value of personal data.

Subsequently, users are more savvy about the type of consent they give for the use of their data, the level of data protection provided by businesses and what steps they can take if their data privacy rights are breached. Are done.

As a result, businesses need to not only focus on regulatory compliance, but also work on gaining consumer trust by demonstrating their commitment to protecting personal data.

As this law continues to reshape global data protection practices, it is important for all businesses to not only comply with its legal mandates, but also understand the broader impact of GDPR on the perception of data privacy.

Data Privacy in the United States

In the United States, the data privacy landscape is diverse and complex. Due to the lack of comprehensive federal legislation, data protection laws are constituted by myriad state-level statutes and territory-specific regulations.

Federal Regulations Governing Data Privacy in the United States

At the federal level, several laws regulate specific areas or classes of data. Notable among these are the Health Insurance Portability and Accountability Act (HIPAA) for health information, the Children's Online Privacy Protection Act (COPPA) for children's data, and the Gramm-Leach-Bliley Act for financial institutions.

Additionally, the Federal Trade Commission Act provides the FTC with broad authority to enforce unfair and deceptive practices related

to consumer privacy and data security. However, despite persistent calls and legislative proposals, the United States has not yet passed a nationwide privacy law similar to the GDPR in Europe.

State-level Contributions to the Complexity of Data Privacy Laws in the US

In the absence of comprehensive federal legislation, individual states have also enacted laws contributing to the complex nature of data privacy regulation in the US.

California has been leading the way with the introduction of the California Consumer Privacy Act (CCPA) in 2018. It provides California consumers with expanded privacy rights and control over their personal data. The implications of the law extend beyond the state, affecting many businesses across the country due to its huge economy. Virginia and Colorado have enacted the Consumer Data Protection Act and Privacy Act, respectively, and several other states have proposed similar legislation.

Main Differences Between American and European Approaches to Data Privacy

American and European attitudes towards data privacy are fundamentally different. While Europe considers privacy a fundamental human right, the American approach is more focused on preventing harm and unfair business practices.

Unlike the broad data protection framework seen in Europe with the GDPR, the US has sector-specific privacy laws. In the US, businesses generally have more flexibility in using personal data for commercial purposes, and consent requirements are less stringent than under the GDPR.

Furthermore, enforcement mechanisms also differ. While US regulators can impose hefty fines for violations, they typically do not have the power to shut down operations or stop data processing, unlike their European counterparts.

This apparent divergence in approaches underlines the need for businesses operating in different sectors to be versed in the nuances of data protection law. Understand each jurisdiction and your obligations thoroughly.

Emerging Trends in Data Privacy

As the digital world continues to evolve and expand, so does the scope of data privacy. From new regulations around the world to advances in technology, a wide range of emerging trends are shaping law and influencing the way business operates.

New and Upcoming Data Privacy Regulations on the Horizon Globally

With greater focus on data privacy globally, countries around the world are introducing stricter data privacy regulations. For example, India is planning to enact the Personal Data Protection Bill – a comprehensive data privacy law that bears close resemblance to the GDPR. China also passed the Personal Information Protection Law (PIPL), considered its first comprehensive data protection law.

In addition to individual countries, regions are also developing harmonised legislation such as the African Union's Convention on Cybersecurity and Personal Data Protection. Additionally, in light of the invalidated Privacy Shield Agreement, a new agreement regarding data transfers is also being negotiated between the EU and the US.

These upcoming rules outline a global trend towards greater regulation of data privacy, reflecting key principles of the GDPR, even in traditionally less regulated markets.

Impact of Technological Advances on the Development of Data Privacy Laws

Technology is evolving rapidly, opening up new frontiers of data collection that existing laws cannot fully address. Internet of Things (IoT) devices, artificial intelligence (AI), cloud-based services, and biometric technologies generate large amounts of data, often sensitive, increasing the potential for big data analytics and personalised marketing, but privacy risk also increases.

These advanced technologies, while beneficial, often involve extensive data collection, processing, and sharing, increasing the potential for unauthorised access and data breaches if not properly managed. Emerging technologies such as blockchain also present unique data security challenges, particularly around the rights to data rectification and erasure under laws such as GDPR.

As a result, these technological advances require regular updates

to data privacy laws to ensure they keep pace with industry advances, protect consumers, and prevent potential abuses.

Industry-Specific Considerations in Emerging Data Privacy Regulations

While data privacy rules apply across the board, some emerging laws include industry-specific provisions. For example, layers of regulation may be added to sectors that handle more sensitive data, such as healthcare, finance, or services that deal with children's data.

For example, the GDPR has strict consent requirements for the processing of sensitive personal data. Other laws, such as HIPAA in the US, apply specifically to health care institutions, setting strict rules regarding patient data. The US state of Maine also passed a law specifically targeting Internet service providers.

Regulators are increasingly recognizing that basic security should apply to all personal data, but some industries, due to the nature and extent of the information they process or the demographics they serve, may require additional safeguards. May be required.

Digital Data Protection under Indian Legal Framework Toward Right to Privacy

"If the right to privacy means anything , it is the right of the individual, married or single, to be free from unwarranted governmental intrusion."

-William j Brennan

In INDIA right to privacy is constitutionally protected as being a part of 'right to life' under Article-21 of the constitution of India. But so far as regards the digital protection of right to privacy protection of Article-21 become less effective because Technology has provided endless possibilities to human beings of development, but on the other hand it has posed numerous challenges in front of us.The advancement of innovative technologies and wide use of the internet, it became very easy to access anyone's data and share such data with a third party which may lead to misuse of data.

Information Technology Act, 2000 and The Digital Personal Data Protection Act,2023 are existing legislation in the country that keeps the privacy of an individual protected in the matters of Data and Information transactions. The I.T. Act was amended in the year 2008 by the Indian legislature and added several provisions to the existing Act of 2000 to make them more effective in the field of protection. The

Information technology Act and the Amendment Act 2008 have the following provisions that ensure the privacy in the Data related issues such as:

- **Section 30**- Section 30 of the Information Technology Act, 2000 needs the certifying authority to conform to safety processes to guarantee electronic signatures secrecy and privacy.
- **Section 43-** Section 43 of the Information Technology Act, 2000 provides sufficient provision for the person concerned to receive compensation for unlawful access to his private and personal data.Under this section intrusion of one's computer or computer framework amounts to compensation. Several clauses and explanations of this section were amended by the ITAA 2008 which are clause (a), clause (i), clause (j), and explanation (v).
- **Section 43A** (by ITAA, 2008) - This completely new section was added to the statute through the IT Amendment Act 2008. This section provides 'Compensation for inability to safeguard data- where an entity that possesses, distributes or handles any delicate private data or information in a computer resource that it possesses, monitors or works is negligent in applying and retaining appropriate safety practices and procedures and thus creates any individual unfair loss or unfair benefit, that entity is responsible to pay the losses by the way of compensation to the person who is affected.'
- **Section 66-** Section 66 of the Information Technology Act, 2000 also protects sensitive private information residing in a computer resource as it makes, among others, a punishable decrease in the value of information residing within a computer resource with imprisonment for up to three years. Thus, if an attacker is hacking into the computer system and copying and transferring sensitive personal information to a rival that may be of very high utility or of very private nature or business importance to the proprietor, the said act results in a decrease in the amount of data located within a computer resource and thus infringement of privacy.
- **Section 72** - Section 72 of the Information Technology Act, 2000 says about violation of confidentiality and privacy, i.e. a government officer can be fined if he transfers in his formal ability any digital information or data which he has obtained about a person. There is only a limited implementation of this section. It is confined to the actions and omissions of those individuals who

have been given authority under this Act, rules or laws produced under it, i.e. police, certification authorities and officials approved by particular notice.

- **Section 72A**- This section was also added to the statute through I.T.Amendment Act, 2008. Section says; Punishment for disclosure of information in breach of a lawful contract - Save as otherwise provided in this Act or any other law for the time being in force, no person, including an intermediary, who, while providing services under a lawful contract, Accessing any material containing information about another person, without the consent of the person involved or in breach of a lawful agreement, with the intention of causing unlawful harm or unlawful gain, or with the knowledge that he or she is likely to do so Should be done, such work will be punished. Probation up to three years or fine up to Rs 5 lakh or both.

Justice B.N. Srikrishna, a retired Supreme Court judge, was set up by the Ministry of Electronics & Information Technology in July 2017 to help frame data protection norms. The recommendations of this committee, in turn, were based on major regulatory developments that were popular while the work of the committee was proceeding. Primary among these was the European Union's (EU's) General Data Protection Regulation (GDPR). While the general preventive framework of the 2019 bill was welcome, its expansive scope was problematic. It created a number of significant compliance requirements that would have affected both big and small firms in the economy. It also proposed the creation of a DPA that had significant regulation-making and supervisory powers. These regulations would have further detailed the already significant compliance requirements in the bill.

The DPDP[Digital Personal Data Protection Act] Act 2023 is based on the draft proposed by the government in November 2022, which adopted a radically different approach to data protection regulation. Compared to the 2019 version of the bill, the DPDP Act, 2023 is more modest—it has reduced obligations for businesses and protections for consumers. On the one hand, the regulatory structure is simpler, but on the other, it vests the central government with unguided discretionary powers in some cases.

The 2023 act allows personal data to be processed for any lawful purpose.The entity processing data can do so either by taking the concerned individual's consent or for "legitimate uses," a term that has been explained in the law. The Digital Personal Data Protection Act-

2023 propose some significant importance to protect the digital privacy which are as follows:

Purposes of Data Collection and Processing

Consent must be "free, specific, informed, unconditional and unambiguous with a clear affirmative action" and for a specific purpose. The data collected has to be limited to that necessary for the specified purpose. A clear notice containing these details has to be provided to consumers, including the rights of the concerned individual and the grievance redress mechanism. Individuals have the right to withdraw consent if consent is the ground on which data is being processed.

Rights of Users/Consumers of Data-Related Products and Services

The DPDP Act also creates rights and obligations for individuals. These include the right to get a summary of all the collected data and to know the identities of all other data fiduciaries and data processors with whom the personal data has been shared, along with a description of the data shared. Individuals also have the right to correction, completion, updating, and erasure of their data. Besides, they have a right to obtain redress for their grievances and a right to nominate persons who will receive their data.

Obligations on Data Fiduciaries

Entities responsible for collecting, storing, and processing digital personal data are defined as data fiduciaries and have defined obligations. These include: (a) maintaining security safeguards; (b) ensuring completeness, accuracy, and consistency of personal data; (c) intimation of data breach in a prescribed manner to the Data Protection Board of India (DPB); (d) data erasure on consent withdrawal or on the expiry of the specified purpose; (e) the data fiduciary having to appoint a data protection officer and set up grievance redress mechanisms; and (f) the consent of the parent/guardian being mandatory in the case of children/minors (those under eighteen years of age).

Moderation of Data Localization Requirements

The 2023 law reverses course on the issue of data localization. While the 2019 bill restricted certain data flows, the 2023 law only states that the government may restrict flows to certain countries by notification. While this is not explicit, the power to restrict data flows seems to be to provide the government necessary legal powers for national security

purposes. The law also states that this will not impact measures taken by sector-specific agencies that have or may impose localization requirements.

Exemptions From Obligations Under the Law

The law provides exemptions from consent and notice requirements as well as most obligations of data fiduciaries and related requirements in certain cases: (a) where processing is necessary for enforcing any legal right or claim; (b) personal data has to be processed by courts or tribunals, or for the prevention, detection, investigation, or prosecution of any offences; (c) where the personal data of non-Indian residents is being processed within India; and so on.

New Regulatory Structure for Regulating Data Privacy

The 2023 law completely changes the proposed regulatory institutional design. The 2019 bill proposed an independent regulatory agency. The DPA was proposed on the lines of similar government agencies in many EU countries that function independently of government and implement the GDPR. The proposed Indian DPA was arguably more powerful since it was proposed to have much more extensive regulation-making powers than DPAs under the GDPR. In addition to framing regulations, the DPA would have been responsible for framing codes of conduct for businesses, investigating cases of noncompliance, collecting supervisory information, and imposing penalties on businesses.

Finally, the 2023 law contains a novel provision not included or discussed in any previous version. Section 37 of the Digital Personal Data Protection ACT,2023, which allows the government, based on a reference from the board, to block the public's access to any information that enables a data fiduciary to provide goods or services in India. This has to be based on two criteria:

- the board has imposed penalties against such data fiduciaries on two or more prior occasions, and
- the board has recommended a blockage. The government has to provide the data fiduciary an opportunity to be heard before taking such action.

Judicial Precedent in Protection of Right to Digital Privacy

Even though in most of the cases, courts didn't explicitly recognise the right to privacy, the highest court of the country ruled in favour of the existence of the right in the landmark decision of ***K.S.Puttaswamy vs. Union of India***[1] The decision delivered in 2018 by a 9 judge bench read the right to privacy within the ambit of Article 21, which is the right to life and liberty. In declaring that the right to privacy is intrinsic to life and personal liberty, the Court overruled earlier decisions of MP Sharma[2] and Kharak Singh[3] held that privacy wasn't protected as per the Indian constitution. The Bench declared the following in the decision:

1. The recognition of the right to privacy in no way means amending the Constitution or granting a new freedom; it is just the interpretation of already existing provisions.
2. Privacy aims to protect personal intimacies, sanctity of personal life, marriage, reproduction, sexual orientation, etc.
3. Privacy also means the right to be left alone.
4. Just because a person sets out his foot in a public place doesn't mean he surrenders all his rights to privacy. It is attached to a person, no matter where he is or goes.
5. The Constitution must be interpreted liberally to allow growth and development with technological changes.
6. However, even though the right to privacy is a basic right, it's not an absolute right. Like every other fundamental right, it also has a set of reasonable restrictions imposed upon its usage.
7. Privacy has both positive and negative connotations. The negative part restricts the state from doing any act that may violate an individual's right to privacy and the positive connotation denotes the proactive duty imposed on the state to protect the right to privacy.
8. The recognition of the right to privacy as a fundamental right protects the inner sphere of an individual from interference by state and non-state actors.
9. The right to privacy can't be denied, even if there's a tiny fraction of people who are affected by it.

1. 2017 10 SCC1.
2. AIR 1954 SC 300,304.
3. AIR 1963 SC 1295.

Unique Identification Authority of India vs. Central Bureau of Investigation[4]: The court in this fascinating case decided on the issue of whether collection of biometrics by the UIDAI without the consent of the person violated the right to privacy. The court upheld the constitutionality of the Aadhar but also imposed certain restrictions on the data collection to allow people to safeguard their privacy. The decision assumes even more significance as it tries to maintain a delicate balance between the aim of the government with that of an individual's privacy rights.

The significance of the right to privacy can also be seen in the decision of **Joseph Shine vs.Union of India**[5] where the Apex Court decriminalised adultery mentioned in Section 497 of the IPC. Justice Chandrachud, writing the concurring opinion on the subject matter, stated that Section 497 criminalises adultery that was put in place to reinforce the idea that in marriage, a woman loses her autonomy and agency. She loses her own identity and is restricted to the patriarchal norms of society. J. Chandrachud employed the concept of right to privacy in deciding to decriminalise adultery as an offence.

In a recent case of **X vs. The Principal secretary, Health and Family Welfare Department, Govt.of Nct of Delhi & Anr.**[6], rendered by the Apex Court, the reproductive autonomy of an unmarried woman was upheld. As per the facts of the case, the Bench permitted a 25 year old woman to undergo abortion as her right to bodily autonomy is guaranteed in Article 21 of the Constitution. The right to privacy enables a person to exercise bodily autonomy under Article 21.

Internet Freedom Foundation vs. Union of India[7] Considered to be another landmark decision in the realm of the right to privacy, the case dealt with the issue of internet shutdowns and how they impact the right to privacy. The Supreme Court held that the suspension of internet services is against our fundamental rights and must not be permitted unless they adhere to the principles of necessity and proportionality.

The cases mentioned above highlight the evolution of the right to privacy in the Indian context. These decisions reflect how the right to privacy has adjusted to different societal concerns, technological advancements and constitutional values. As can be seen from the start, there was indeed an absolute resistance to recognise the right to

4. Laws [SC]-2014-3-100 .
5. AIR 2018 SC 4898 .
6. Civil Appeal No.5802 of 2022[Arising out of SLP[C] No.12612 of 2022].
7. Writ Petition [c] No.44 of 2019.

privacy, as it didn't find an explicit place in the Indian constitution. But overtime, the judiciary, speaking through different Benches, underlines the role of the right to privacy in one's right to life and personal liberty enshrined under Article 21. It can't be doubted that as we go forward, there will emerge more and more technological challenges and to face them head on, these decisions will go a long way in guiding us towards a better and more secure future.

Conclusion

In today's time, our personal information is required for security purposes. We all provide the authentic institutes the specified information that is asked by them. It is provided on a trust basis that our information is in the safe hands and will not be given to any unknown person without our knowledge. Though, the notorious netizens have become so smart nowadays that they can acquire our personal information, which were not supposed to be leaked, by using there, so-called hacking skills. Such netizens in India, are not even afraid of committing such offences since they know that laws are not properly framed yet, and also if they get caught, they won't be punished strictly. It is a need of the hour that proper Data Protection laws are made, so that the citizens of the country are not under a constant fear of their personal details getting leaked and getting misused. It is also necessary for us, so that foreign companies who are willing to enter the Indian market are not afraid of doing so since no company would ever invest its time and money in a country which is vulnerable to its data and privacy protection.

◆ ◆ ◆

9.

Digital Consumer's Confidentiality and Artificial Intelligence: An Analysis

Mrs. R. Vimala

What is Artificial Intelligence?

Artificial intelligence (AI) is the ability of machines to execute activities that need human intelligence, but there is no one, precise definition for this term[1]. They execute cognitive tasks, grow in capability, and learn from experiences. They are able to mimic some mental processes of humans, such as linguistic interaction, learning, and problem-solving[2]. AI was created to support humans in making sophisticated decisions and completing difficult jobs. Our lives become easier and more comfortable as a result of the reduction of hard human labor. Large-scale data integration with clever algorithms is how artificial intelligence (AI) works, enabling software to recognize patterns. It synthesizes data from several sources, analyzes it, and generates an interpretive result. Neural networks, machine learning, deep learning, cloud computing, and other key elements of

1. Artificial Intelligence, Built In, https://builtin.com/artificial-intelligence.
2. H. Steering AI and advanced ICT's for knowledge societies: Rights, Openness, Access, and Multi-stake holder Perspective, 10(1st ed., 2019)

***Assistant Professor, VELS School of Law VELS Institute of Science and Technology and Advanced Studies VISTAS**

AI.Recognition and computer vision using natural language. Artificial General Intelligence and Narrow AI are the two main categories into which AI has been extensively separated. When it comes to narrow artificial intelligence (AI), one goal must be completed successfully, but the AI is limited and unable to do even simple tasks like weather prediction. Currently, these are used more frequently, althoughStrong AI, often known as artificial general intelligence, is intelligence that is similar to human general intelligence but is applied to activities such as advanced robotics. Over the years, artificial intelligence has grown dramatically on a global scale. By 2023, it is predicted to increase to 99.94 billion dollars at a compound annual growth rate of 34.86%3. Three. According to estimates, the AI market in India was worth 6.4 billion dollars as of July 2020. It is anticipated to increase significantly over the next several years and significantly boost the nation's GDP4. To assist with duties and reduce the workload of human labor, artificial intelligence (AI) has been implemented in a number of market areas, including the health care and business organizations.Shopping on the web Additionally, companies have developed AI virtual assistants like Siri, Google Assistant, and Amazon Echo that help customers complete tasks5. Voice commands allow users to command these virtual assistants to do a variety of functions, such as playing music, obtaining information, reminding them of deadlines, controlling smart home devices, reading the news to them, and more. Similar to this, wearable technology—such as fit bits and smartwatches—uses artificial intelligence (AI). People utilize these gadgets as healthcare aids since they can monitor their heart rates, track how long they sleep for, and receive health advice, among other things. Because AI is capable of performing a variety of tasks, hence due to this character of AI it has been welcomed all across the world and in future, it is expected that its performance will be more versatile and accurate. All over the world businesses have largely adopted the use of AI. The main purpose is to improve their consumer experiences and maintain their consumer base. With Artificial Intelligence, business organizations aim to provide their consumers with quality experiences and at the same time collect consumer data through personal questions or recording of browsing

3. Global AIMarket Report(2020-2030)-Covid-19 growth and change, GlobeNewswire (June 4, 2020), https://www.globenewswire.com/news- release/2020/06/04/2043624/0/en/Global-Artificial- Intelligence-Market-Report-2020-to-2030-COVID- 19-Growth-and-Change.html#:~:text='The%20global%20artificial%20intelligence%20market%20is%20expected%20to%20grow%20from,(CAGR)%20of%2043.39%25,

4. Siddhartha Thomas, State of AIin India 2020, AnalyticsIndia Magazine(Sept. 8, 2020), https://analyticsindiamag.com/report-state-of- artificial-intelligence-in-india-2020/.

5. What a Virtual assistant is and how it works, Lifewire, availableathttps://www.lifewire.com/virtual- assistants-4138533.

habits to attract consumers.

The Influence of Aggregators on Consumers' Intent to Purchase

Producers, distributors, and consumers make up the bulk of the market's distribution route. The role aggregators[6] is a new distribution channel that falls within the indirect distribution channel. Huge internet marketplaces that house several service providers under a single brand name are referred to as aggregators[7]. These platforms come in the form of mobile applications or websites. Examples of such platforms include Amazon, Uber, Swingy, and others. They link directly with consumers and offer a variety of items from various service providers, including local vendorsname only[8].Intent-based marketing, which entails promoting a good or service based on each customer's unique interest and intent to buy, as seen by their browsing and purchasing behaviors, is the main focus of these aggregators[9]. In order to comprehend what their customers search for on other websites or other platforms, it also relies on external data. These commercial companies gather a tonne of customer data from users' general activity on related platforms in addition to their platforms[10]. To better serve the unique demands of each of their customers, they further turn these data into valuable commodities. For instance, Netflix makes movie recommendations based on user viewing history. In a similar vein, Amazon makes product recommendations based on user browsing habits and past purchases.

Additionally, they have developed tactics like order dispatch. Before the customer placed an order, they already ship the item. This is how Amazon operates for its Amazon Fresh and Amazon Prime products. Using artificial intelligence, it predicts product demand based on customer interest and purchase intent in a given area. The groceries or prime products are then pre-stocked in the area's warehouse and are delivered to customers within a few hours of their order[11].Amazon can draw in considerably more customers and grow its customer base than

---

6. Typesofdistributionchannel,EconomicsDiscussion,https://www.economicsdiscussion.net/distribution-channel/types-of-distribution-channels/31760.

7. The Aggregator model- rise, challenges, and scope of thisapproachinIndia,First Post, https://www.firstpost.com/business/biztech/the- aggregator-model-rise-challenges-and-scope-of-this- approach-in-india-3728527.html.

8. Ibid

9. What is Intent based Marketing and why is it important,Markle tic,available at https://www.markletic.com/blog/what-is

10. Ibid

11. Dave Chaffey, Amazon.com marketing strategy: A business case study, Smart Insights, available at https://www.smartinsights.com/digital-marketing- strategy/online-business-revenue-models/amazon- case-study/.

its rivals thanks to its rapid delivery system and the extra advantages of the Amazon Prime Subscription. This is an illustration of how data aggregators such as Amazon use artificial intelligence to gather personal customer information and turn it into valuable commodities for their own profit.

Notion of Entity Resolution Along with Ways to use it to Convince Customers

In their daily lives, people reveal their credit/debit card information, location, and hobbies through a variety of activities such as browsing through several social media platforms, making online purchases, and so on. Artificial Intelligence enables businesses to store this data as customer points, which can then be used as touchpoints to target customers by presenting them with personalized products based on their interests and promoting products they are likely to buy. This gives customers an incentive to choose their brand over rivals[12].Everywhere there is a customer, there is so much data collected daily that technologies like Google Analytics integrate and store all of the consumer data points through an analytical model called Entity Resolution[13], with the assistance of data from various external data collection firms.Using this strategy, businesses can better understand the unique preferences and choices of each customer and offer items that align with those decisions, as well as support political campaigns and other relevant advertising. For instance, in the now-famous Cambridge Analytica case, Facebook[14]assisted the political consulting firm Cambridge Analytica in obtaining personal information from the profiles of approximately 87 million Facebook users. Cambridge Analytica was involved in Donald Trump's presidential campaign in 2016. Facebook acknowledged that it had given Cambridge Analytica access to the personal information of 87 million users, which was then utilized for Donald Trump's campaign[15]. Through a Facebook personality quiz, the users' interests, location,

12. 20 consumer touchpoints that will optimize your consumerjourney, HubSpot,availableat https://blog.hubspot.com/service/consumer- touchpoints.

13. Entity Resolution: Key to creating a master data framework, Dun & Bradstreet, https://www.dnb.com/perspectives/master- data/business-entity-resolution-with-master-data- management.html#:~:text=Entity%20resolution%20i s%20the%20 process,person%2C%20or%20other%20 data%20type.&text=This%20single%20version%20 of%20truth,from%20growth%20to%20risk%20mitigat ion

14Issie Lapowsky, How Cambridge Analytica Sparked the Great Privacy Awakening, Wired, https://www.wired.com/story/cambridge-analytica- facebook-privacy-awakening/, The Facebook and Cambridge Analytica scandal, explained with simple diagram, Vox, availableat https://www.vox.com/policy-and- politics/2018/3/23/17151916/ facebook-cambridge- analytica-trump-diagram,.

15. Ibid

favorited pages, preferences, intention to buy, and other details were captured in order to determine the users' political leanings. Potential voters were swayed and coerced to cast as many votes in their favor with the aid of this. Not how Cambridge Analytica helped with the campaign, but how a massive platform like Facebook disclosed user data of millions of people without permission is the topic at hand. Facebook receives a lot of data from users in their daily lives. Uploading photos and sharing where they are, what they've been, and who they are individually selections, and other information are all saved by Facebook, which monitors user activity. Second, it allows users to deactivate their accounts rather than permanently deleting them. This implies that even after doing so, their data and past activities will remain saved, indicating that even if users would like to delete all of their data, they choose not to. Thirdly, Facebook keeps more data than is shared on its platform since it permits users to connect in to third-party programs, which enables it to monitor user activity on other networks. With the use of AI, all of these data are gathered through games, quizzes, favorite pages, and other activities.

India's Digital Market Scenario

According to studies, the Indian e-commerce business is expanding more quickly than other countries. By 2026[16], it is predicted to reach $200 billion and have 850 million users. By 2034[17], it is forecast to overtake the US market to rank as the second largest e-commerce market globally. The vast internet marketing campaigns and campaigns that these corporate behemoths have embraced are to blame for the paradigm shift from offline to online consumerism, which has opened up new ground for consumer expectations[18]. Online shopping is handy and time-saving for consumers, since it guarantees them speedier and less expensive services. Moreover, consumers are encouraged to interact with these platforms more since they may purchase high-quality products at a reduced cost during significant online events like Amazon's Great Indian Festivals and Flipkart's Big Billion Sale. Then, features like voice search and the ability to search via images in local languages have drawn the interest of Indian customers and made online shopping easier for them. Subscription services and other loyalty programs have also assisted e-commerce in building a loyal customer base by offering

16. Ecommerce Industry in India, India Brand Equity Foundation,(Dec4;2020),https://www.ibef.org/industry/ecommerce.aspx.

17. Bain and Flipkart foresee 350 million online shoppers by 2025, Consultancy.in, (June 29, 2020), https://www.consultancy.in/news/3139/bain-and- flipkart-foresee-350-million-online-shoppers-by- 2025.

18. Supra 16.

them individualized services that make them feel valued and keep them returning to their websites.This indicates how these commercial entities have penetrated the Indian market and established a more secure position for themselves in the online marketplace. With the use of artificial intelligence (AI), they have been able to comprehend Indian culture and have developed methods tailored to the needs of the Indian market. Consequently, it can enter Indian markets. Customers have developed a strong attachment to the platforms that readily provide these companies with their personal information, which they then use into invaluable assets for their operations.

Digital Customers' Challenges

E-commerce and online platforms are incredibly potent, and they greatly influence how consumers behave. They gather a great deal of data on their customers, both through cookies and other means, making it simple for them to trick them into making purchases or using services they otherwise might not have. As these Fake messages on websites convey to users that a product is performing well and that if they don't buy it, other customers will take it. This is how websites continuously sway users' interests. Despite their better judgment, these messages encourage customers to make impulsive purchases. The opt-out of service link is hidden in the drop-down menu or somewhere else that is difficult to see, and they employ techniques like brightening the availing of service button to draw in customers. Furthermore, people find it challenging to fully give up on popular digital platforms like Facebook, which has bought other social media sites like Instagram, WhatsApp, and so on.In addition, customers worry that if they stop using the site, they might lose all of the connections they have formed through it.[19] because there aren't any safer options available. Instead of making a new account every time they visit a new website, many users find it more convenient to log in using their Facebook account on third-party apps. Offering a plethora of incentives, such as expedited shipping, discounts, and customised products, among other things, helps platforms like Amazon retain and attract customers. This builds their trust and makes it impossible for them to defect without exerting a great deal of personal effort[20]. The conversation above makes it very evident that major online platforms have established themselves throughout the digital industry, and since there aren't any other safer options, users will inevitably choose these platforms. Furthermore,

19. Bhaskar Chakravoti, Why it's hard for users to control their data, Harvard Business Review, (Jan 30, 2020), https://hbr.org/2020/01/why-companies-make- it-so-hard-for-users-to-control-their-data.

20. Ibid

since the advent of the Internet of Things, businesses are able to monitor each and every move of their This gives them a good deal of leverage over their customers' decision-making processes when it comes to making purchases and piqueing their interest in specific goods and services. It is difficult for consumers to make informed decisions in the digital market because of the extent to which these internet platforms govern them. It's clear from this how much power and influence these internet platforms have on users, creating an ecosystem that is out of balance for users.

Legal Perspective

Consumer Protection Act 2019

The number of digital consumers is rapidly increasing in this day and age of commerce and digital marketing, yet with such rapid expansion comes a plethora of issues for consumers[21]. Therefore, the Government of India passed the Consumer Protection Act, 2019 to particularly address the difficulties of digital consumers together with other consumer protection issues, with the goal of creating a safe environment for these customers. This Act addresses and imposes strict accountability on electronic service providers in addition to replacing the old Consumer Protection Act of 1986, which exclusively addressed offline or marketplace consumer disputes.The Central Consumer Protection Authority, which is empowered by the Central Government to impose penalties and other reasonable measures, is the grievance mechanism established to address any disputes pertaining to consumer protection. A proper procedure for filing complaints regarding any dispute has been established. A commission for consumer dispute resolution will thereafter be established in each state and district to handle complaints from consumers at the state level.

The Consumer Protection Act of 2020 includes six rights for consumers: (i) protection from the marketing of products and services that endanger life and property; (ii) information about the quality, quantity, potency, purity, standard, and price of goods and services; (iii) guaranteeing access to a wide range of products and services at reasonable prices; and (iv) recourse against unfair or restrictive trade practices22. This act updates India's consumer protection laws, making them more progressive and facilitating speedier delivery of justice. The Government of India also introduced the Consumer Protection

21. Section 7(ii)(b), Consumer Protection Act,2019.

22. The Consumer Protection Bill 2019, PRS legislative Research.https://www.prsindia.org/billtrack/consumer- protection-bill-2019.

(E- commerce) Rules, 2020 to supplement the Consumer Protection Act 2020. It defines the obligations and responsibilities of e-commerce platforms, strives to increase transparency and information disclosure by these platforms to customers, and outlaws unfair trading practices in the online marketplace[23]. By enacting these two Acts, the Indian government hopes to establish a fair and stable marketplace that benefits both buyers and sellers. This would allow the country's digital market to expand and possibly boost GDP.

Personal Data Protection Bill 2019

The Lok Sabha was presented with the Personal Data Protection Bill 2019 with the specific goal of safeguarding the personal information of individuals. The bill covers all businesses falling under its purview and applies to data processing by the government, foreign companies, and companies incorporated in India. It classifies some information as important personal data[24]and some information as sensitive personal data, including financial information, biometrics, political opinions, and information on religion or politics. It gives the consumers or individuals whose data is being processed the ability to request information about how much of their personal data is being processed, to have inaccurate or incomplete personal data corrected, to have their data erased, and—above all—to emphasize the importance of giving consent.A person can no longer have their data used by businesses or other relevant bodies if they withdraw their consent to have their data transferred or processed. This compels all companies to obtain user consent before to processing or transferring personal data and mandates organizational reforms to improve data protection across the board. The measure mandates that social media intermediaries with a large user base implement a voluntary user verification process for users in India[25].All sensitive and vital personal data must be stored in India alone, according to the bill, and cannot be sent to any other nation. Only when it satisfies rules akin to those under the General Data Protection Regulation can sensitive personal data be transferred outside of India. In order to safeguard people's interests, stop data misuse, maintain openness, and guarantee legal compliance, this measure also calls for the creation of a Data Protection Authority. It contains the provision that the government may request to share with business entities any important non-personal data. Additionally, it specifies penalties for anyone found to be in violation of any legal provisions. The government hopes to safeguard

23. Consumer Protection Ecommerce Rules,2020.

24. Ibid

25. Supra note 24.

citizen privacy and stop commercial entities from abusing their data by enacting this measure.

Way Ahead

The Way Ahead It is an undeniable reality that technology has taken over as the primary method of communication in the modern world, and that this trend will only continue. This implies that the number of digital platforms and online users will rise. Thus, the Government and Business Organizations at their levels need to recognize the value of data and provide a safer marketplace for customers in order to keep the market in balance.

Government

Authorities By 2022, the Indian digital economy is predicted to grow to a trillion dollars. This implies that there will be more e-commerce platforms and a consequent increase in the amount of data that is accumulated. The Personal Data Protection Bill was created by the Indian government in an effort to safeguard, regulate, and stop the exploitation of the data belonging to its citizens. The government also hopes to enforce legal compliance on all firms who conduct business in India. This bill is a step in the right direction toward improving openness and protecting citizen data. Additionally, it prohibits the use and transfer of private data without the user's permission.As citizens now have a fundamental right to privacy and the ability to revoke, amend, and remove any personal information they have given to organizations, the government emphasizes the need of consent. The Government is freed by the Bill from its jurisdiction to gather data for official purposes. For example, the Unique Identification Authority of India saves the Aadhar information of every Aadhaar cardholder. The Central Monitoring System, the National Social Registry, and other agencies monitor data for various purposes. The government gathers and retains data for these objectives. The government has authorized the collection and storage of data by these agencies because it is necessary for the citizens' well-being.The bill's drawback is that it exempts agencies from liability. Despite the fact that data is gathered for the aim of maintaining a database on the citizens and their welfare, these agencies ought to inform the public about the ways in which their data will be utilized. Recently, Covid-19 awareness has been raised with the Arogya App.By using this app, citizens had to give the central government access to their personal information. However, doubts persist among the public over the duration for which the data would be retained, the identity of the creator of the application, and the organizations to whom it will be

accessible. Citizens expect the government to comply with the Right to Information Act 2005 (henceforth referred to as RTI) and supply them with the appropriate information in these kinds of situations. To improve the government's accountability for responding to public inquiries, the Right to Information Act was introduced. According to others, it also works in tandem with privacy laws, as they both aim to increase government transparency and accountability to the people.

Even though the RTI Act was greeted with enthusiasm, it appears that it is progressively fading away. According to statistics, between 40 and 60 lakh RTI applications are filed annually, yet fewer than 45 percent of those applicants receive the information they requested30. The State Information Commission is now handling 2.18 lakh appeals and complaints. Applications pertaining to questions about demonetisation and the most recent PM-Care fund for the Covid-19 pandemic have also been turned down by the government[26]. Citizens perceptions of government actions are clouded by rejection of applications and a lack of responsibility on important issues, which is one of the reasons less RTI applications are being filed[27].These days, the government must also develop policies for its agencies in order to guarantee that citizens' rights to information are upheld and their legitimate concerns are addressed. in order for them to feel secure knowing that their data is protected by the government. Additionally, this will guarantee greater accountability and transparency from the government. Additionally, the government may incorporate more stringent regulations that are advantageous to India by citing other nations' privacy laws, such as the GDPR.A move in the right direction, the Consumer Protection Act of 2019 will enable the government to maintain strict regulation over digital marketplace platforms and to make the digital consumer environment safer. Moreover, the government has to guarantee that businesses and other authorities appropriately abide by the laws it has passed.

Business Organisation

Customers are shifting their purchasing habits from physical to online markets due to the increasing volume of e-commerce on digital platforms[28]. Customers now have a variety of platforms and possibilities to choose from at the same time. As a result, there is constant competition

26. K. Satish Kumar, The paradox of our rights to information and privacy, live mint , (Dec 11, 2019), https://www.livemint.com/opinion/online-views/the- paradox-of-our-rights-to-information-and-privacy- 11576085219492.html.

27. Ibid

28. Supra 12

among various platforms to draw in a larger audience. Customers are gradually growing more conscious of how these platforms use their data in the modern era. Through articles and documentaries, people are becoming aware of how they are being tricked into giving personal information that could pose a risk to them. Customers are becoming more perceptive and cautious with their data as a result.It is therefore important for businesses using digital platforms to reassure their customers that the data they submit is secure and won't be misused in order to keep them as customers. By guaranteeing that their data is secure and that not even Apple can access it, Apple, for instance, gained the faith of its customers in the Federal Bureau of Investigation-Apple Encryption debate. Following this, it was successful in drawing in and keeping more customers.

Attack on Bernardino [29].Apple declined to decrypt because they lack the necessary feature. In order to accomplish this, the FBI filed a lawsuit asking the court to require Apple to develop a special operating system that would enable hackers to disable the most important security protections of iPhones. Apple objected to the order, claiming that it was illegal and may jeopardize the security of all of its users' data.Tim Cook, the CEO of Apple, maintained his position, and as a result, the business received a lot of support from its users and, in the end, was able to acquire the trust of the general public. As a result, even though Apple products cost more than those of other brands on the market, their increased level of trust attracts more customers. This is an illustration of how businesses may win their customers' trust by being honest and open with them. Businesses should make adjustments to guarantee that the data of their customers is better protected.In order to protect the valuable information found in the original consumer data obtained and to lessen the chance that privacy will be violated by intruders, they ought to implement the disturbed process. Companies can also combine the original data with additional data to create the synthesized data needed for marketing, protecting the original data and avoiding information loss. It is imperative that they inform their customers about the organization's data processing procedures and security measures.To stop fraud and scams, businesses should offer safe and secure payment methods and collaborate with secure platforms for payments. Before using customer data for any significant objectives, they ought to think about getting agreement from them. Lastly, they ought to take steps

29. Leander Kahney, the FbI wanted a back door to iPhone. Time Cook said no, Wired, (April 16, 2019), https://www.wired.com/story/the-time-tim-cook- stood-his-ground-against-fbi/., Apple vs. FBI, concerning an order requiring Apple to create custom software to assist the FBI in hacking a seized iPhone, https://epic.org/amicus/crypto/apple/.

to make sure that their personal customer data is not being misused. Educating others on the use of single sign-on authentication is another crucial step.

Single Sign-on for Authentication

An internet tool called single sign-on authentication enables users to sign in to numerous sites with just one login, which consists of a username, login ID, and password. This will streamline the login procedure and provide an additional degree of security. Since this solution would lower the security risks for customers and vendors, it will assist businesses in managing privacy on their platforms. Businesses can make their identity protection stronger. By creating a single, strong password that they can use across several platforms, users may minimize password fatigue and streamline the password management process.

Consumer Awareness: An Empirical Study and Analysis

I carried out an empirical survey40 to ascertain customer awareness. Twenty people in various age groups were questioned for the study to find out how knowledgeable they were about data privacy and the rules that govern it. The first thing they were asked was how much time they typically spent online each week. Responses to this ranged from 12 hours per week to all day, every day.When asked what they use the internet for overall, roughly 30% of them said they use it for schoolwork, 30% for pleasure, 5% for online shopping, and 75% for all three. Third, the question of what kind of market they favored and why was posed to them. Because it is more convenient to access, offers high-quality products at discounted prices, saves time, offers a variety of products on one platform, offers a wide range of possibilities, and is simple to exchange, 70% of those who responded preferred the online market over the offline market. They were then questioned with the subject of data privacy. When asked how concerned they are about their security and privacy on these platforms, 50% of the respondents said they are extremely concerned, and 50% said they are slightly concerned but not very concerned. Subsequently, roughly 35% of the total respondents indicated that they had fallen victim to online fraud. Of these victims, 40% said they avoided using the app or website, 40% filed a complaint with the relevant authority, and 10% got in touch with the bank to close their accounts in order to stop losing money.After that, they were asked how many times they refused to give up their personal information. Of those who responded, 40% said they always refused, 50% said they occasionally refused, and 10% said they never refused

to give their personal information to the e-commerce entities. Of those who replied, 85% said they had never been asked for it.In response to questions about why they wouldn't give their data, 55% of respondents said they didn't trust the organizations with their data, 40% said websites requesting personal information don't tell them how they plan to use it, and some said the information requested isn't relevant to the service the websites are offering.After that, they were questioned about the precautions they take to ensure their security and data on these platforms. Some said they use data protection software and antivirus software, verify the legitimacy of websites before using them, only allow data if absolutely necessary, create strong passwords, only disclose bank details on reliable websites, avoid providing personal information or phone numbers on any website, and avoid using the internet altogether. Questionnaires about internet usage and consumer preferences for various market kinds comprised the first section of the study. The bulk of them obviously use the internet frequently and prefer online markets to offline ones based on their comments. The survey findings indicate that consumers are mostly drawn to online markets due to considerations such as cost, time savings, convenience, and versatility, as previously highlighted. Questions about consumer awareness were asked in the second section of the study. While customers are worried about their data privacy and internet security, it has been shown that they do not take significant action to allay these fears.

For instance, the majority of victims of online fraud choose not to use the application or website in instead of making a complaint. This suggests that they may not have known how to make a complaint or may have chosen to avoid using any kind of resolution process because they were uncomfortable doing so. Rather than trying to avoid these types of scams, customers should take the appropriate steps or report the scam online so that the companies are made aware of it and other customers are also made aware of it.The majority of respondents do not provide their personal information because they do not trust the companies with their data and are unsure of how their data will be handled by them. Consumers believe that businesses should be more open and explicit about how they use their data, which suggests that they have little faith in the organizations that request their data.The fact that consumers are aware of their right to know what happens to their personal data and that most of them take steps to protect it on their own are encouraging signs. However, even with these measures in place, it appears that most consumers are unaware of the laws that govern consumer protection and data privacy in the nation.It is

possible that this is because the laws are still in their infancy and that the data privacy bill has not yet been approved, but consumers should remain aware of the laws and know who to complain to about issues pertaining to consumer protection and privacy. This suggests that the government should take significant steps to inform its citizens about the applicable laws on these matters, particularly because internet consumerism is rising in India. It is imperative that customers acquire more consciousness regarding the use of their data on digital platforms and that corporations fulfill their obligation to apprise them of such usage.

Conclusion

As time goes on, the world is becoming more digitalized. The world has become increasingly reliant on technology compared to its past. Human lives have been more convenient and easy with the introduction of numerous technologies, and it is clear that technologies will rule the future. One such technology that has been broadly embraced is artificial intelligence, which I have touched on in passing in this essay. As was previously said, artificial intelligence is highly dynamic and operates much like the human mind does. It can precisely and accurately carry out cognitive activities that call for human intellect. It is accepted in many different domains for just this reason.In order to create individualized products like virtual assistants, smart devices, etc., large firms have also embraced AI. Many daily tasks that make life easier and faster for humans are made possible by these devices. As such, human benefit has been demonstrated by AI advancement. The usage of AI and consumerism is discussed in more detail in the following section of the article. Within this, I attempted to elucidate the ways in which aggregators like as Amazon may shape consumer behavior by devising AI-powered methods to draw in new customers and effectively nurture existing ones. Their competitors have not been able to match their success in the digital industry thanks to strategies like prime delivery and personalized product recommendations.They can also persuade customers to purchase their goods by using aggressive advertising that highlights the excellence of their goods and services. I then went over the idea of entity resolution, which helps businesses comprehend each customer's unique preferences and decisions by storing a variety of personal and political data points about them in a single database. They will be able to increase their customer base and meet the specific needs of each individual.Occasionally, major corporations utilize user or customer data for their own gain. One such instance is when Facebook assisted Cambridge Analytica in the

2016 presidential election by giving them access to 87 million users' personal information. This highlighted the unscrupulous aspect of these massive platforms, which entice users to divulge personal data that these businesses subsequently turn into valuable assets. This clarifies why there are significant hurdles associated with every new advancement. A problem that affects consumers worldwide is the security and privacy of their personal data. Numerous e-commerce platforms are welcome to develop their operations in India, where the digital industry is expanding at a faster pace.A movement of consumers from offline to online markets is occurring as a result of the growth of digital platforms. Because they are easier, more convenient, and save time, most people, according to my empirical research, prefer online markets to offline ones. Additionally, it is true that internet companies have worked to improve its adaptability and convenience for Indian customers. Examples of this include voice search capabilities and search alternatives offered in regional languages. A significant amount of data has accumulated throughout several online platforms, posing a risk to the privacy of users.Customers in India are unaware of their legal rights, in contrast to other industrialized nations like the United States and the United Kingdom where this knowledge is widespread due to low literacy rates. When faced with online frauds or scams, people in the empirical study on consumer awareness mentioned above were shown to do little more than avoid using the application or website in question rather than adopting proactive measures. Not only did most of the respondents know about data security and protection, but the majority also didn't know about the rules that control it.Consumer exploitation and data privacy are serious concerns that cannot be addressed unless customers are also ignorant of their rights. A primary cause of this ignorance was the absence of legislation safeguarding digital consumers. However, with the passage of the Consumers Protection Act 2020 and the Consumer Protection (E-commerce) Rules 2020, the government has addressed this issue by granting online consumers the required protections, relief, and a grievance filing platform. Better security and protection for digital customers are anticipated from this law, which will also stop corporate giants from taking advantage of them.The 2019 Personal Data Protection Bill establishes stringent criteria to safeguard individuals' interests and penalize businesses or e-commerce that violate any of its provisions. This is a good step that will guarantee a better digital consumer ecology and increase their awareness of their rights. Businesses and business associations ought to update their rules to better safeguard customer information, take action to maintain the original data that was supplied to them, and

show greater transparency to their customers . Additionally, with the assistance of non-governmental organizations, the government ought to make sure that businesses abide by the relevant laws and educate the public about consumer protection legislation. Ultimately, the government, businesses, and consumers will all need to work together to establish a better and safer online marketplace. There is no doubting that as people become more accustomed to using technology, the number of digital platforms and the range of options available to them rises.Consumer preference for digital platforms is predicted to grow in the future due to factors including affordability, adaptability, and convenience. The advantages of digital platforms should be emphasized rather than being outweighed by the increased number of issues that come with them. New technology and digital platforms provide many advantages.

◆ ◆ ◆

10.

Impacts of Excessive Digital Device Use

Shahana Parveen P P & Dr. Mahesh MM***

Introduction

In today's digital world, the presence of digital devices has transformed how we live, work, and interact. Smartphones, tablets, laptops and computers are an integral part of our daily routines. These devices offer access to lot of information all over the world, entertainment and communication. Moreover, this digital revolution has also introduced a new form of dependency known as digital addiction, characterized by excessive or compulsive use of digital devices and platforms. These disturbances cause clinically significant disruptions in personal, occupational, and social aspects of life for people who have difficulty disconnecting from their screens (Singh & Singh, 2019). Behaviours due to digital addiction resembles like other substance addiction.

At personal aspect, digital addiction has an impact on one's physical and psychological health. Continuous internet use creates significant mental health issues like, anxiety, depression and attention disorders. Excessive screen time leads to disturbed sleep patterns, sedentary

***Research Scholar, Research and Post Graduate Department of Psychology, Sri.C.Achutha Menon Govt. College, Thrissur, Kerala.**

****Assistant Professor, Research and Post Graduate Department of Psychology, Sri.C.Achutha Menon Govt. College, Thrissur, Kerala.**

life style, eye strain and shoulder pain (Zayed, 2024). The need to stay connected leads to social withdrawal, replacement of face-to-face communication into virtual communication, weakening relationships and quality of social life. Due to decreased concentration and awareness, there will be some trouble in productively involving in academic and professional settings (Zayed, 2024). Addressing digital addiction helps to promote healthier digital device consumption and enhance the well-being of both individuals and society. As internet invades into all areas of a person's life, it creates some specific impact on behaviour, personal, physical, academic, social and relationship.

Behavioral Impact

Excessive use of the internet has become a significant behavioral concern in today's digital world, impacting individual's physical and mental well-being. This overuse can lead to a range of adverse effects. Continuous use of social media can shorten attention span and increase the urge for multitasking, which may reduce overall productivity of a person (Nussenbaum, 2023). Husain et al. (2024) *revealed that there is an association between increased addiction to social networking and aggressive behavior. It concludes that aggressive behavior directly influence increased social network use. Another behavioural impact of overuse of internet use is online grooming. Online grooming is a term used to describe the tactics abusers deploy through the internet to sexually exploit children. Online grooming helps to enhance confidence in young users, so the user can set meeting with them* (Choo, 2009). *The worst result of this kind of meeting is* sexual abuse of victim, physical violence or child prostitution and abuse through pornography. Online grooming generally starts without sexual approach, but designed to tempt the victim to sexual encounter (Choo, 2009).

The pathetic result of online grooming is mainly in the form of physical or sexual abuse. To another extent cyber bullying is a kind of verbal abuse over the internet. Cyber bullying is the use of electronic devices to bully a person, typically sending threatening messages. Due to this behavior individual feels less worthy, loss of confidence, unhappy, frightened and isolated. In some cases it is leads to even suicidal attempt (Bishop, 2013). Suicide or the attempt of suicide because of the internet is known as Cyber suicide. Recently the attention of scientific community turns towards the concept of Cyber-suicide, because the reported incidents of suicide are growing over the internet. Studies related to Cyber-suicide are still in its beginning stage, and there is comparatively less empirical evidence of contribution of internet to suicide attempts. However, the

Internet contains some aspects that lead one to believe that a user can facilitate the act of committing suicide (Biddle et al., 2016). Similar to cyber bullying, cyber racism also involves use of verbal communication related one's race. Cyber Racism refers to racism expressed through online websites. Racism is commonly expressed through internet, but the internet feature of anonymity facilitates its occurrence. Racism can be expressed via racist websites, photographs, films, comments, and messages on social media (Back, 2002).

Excessive internet use leads to internet addiction; currently it is developing as a new type of dependency. It involves symptoms like, compulsive need to spend more time on internet that eventually leads to the impairment of an individual's social, professional, academic or personal functioning (Moreno et al., 2013). Gupta et al. (2018) internet addiction and its mental health correlates among undergraduate college students of a university in North India and he found that the prevalence of internet addiction was 25.3%. Also internet addiction was significantly related with higher family income, greater screen time, always online status, and greater duration of internet use per week. Increased duration of internet use per week and always online status, depression, anxiety and stress were the independent predictors of internet addiction.

Goel et al. (2013) found that 0.7% of Indian adolescents were found to be addicts, and excessive use internet had higher scores on anxiety and depression. Anand et al. (2018) investigated Internet Use Behaviors, Internet Addiction and Psychological Distress among Medical College Students: A Multi Centre Study from South India. They found that among the total 27% of medical students met criterion for mild addictive internet use, 10.4% for moderate addictive internet use, and 0.8% for severe addiction to internet. Internet Addiction was higher among medical students who were male, staying in rented accommodations, accessed internet several times a day, spent more than 3 hours per day on internet and had psychological distress. Predictors of internet addiction involves: age, gender, duration of use, time spent per day, frequency of internet use and psychological distress (depression). They concluded that medical students who have internet addiction will lead to negative effect for their medical education progress and long term career goals. Błachnio et al. (2019) examined the relationships between internet addiction and socioeconomic factors. They conclude that not only personality traits but also the cultural and economic characteristics of the countries where users live can explain the Internet addiction phenomenon.

Internet addiction predicts engagement of electronic gambling (Giotakos et al., 2016). Electronic gambling refers as an activity in which two or more people meet online to exchange bets. This activity involves the risk of financial loss or gain. Loss of money is considered as a major problem, because this will lead to lose one's savings, home or assets etc. many people addicted to this, and they will think that during next round they will get their money back. But this impact not only affects the money of that person, it is also a waste of time. The frequent visit in gambling environment can cause addiction. The easily access to online gambling websites increases the risk of engagement of young adults in such activities (Diomidous et al., 2016).

Similar to the financial loss in electronic gambling, Phishing involves exposing of personal data and information of financial transaction. Every day millions of people conduct electronic transactions and economic activities through internet. Extreme awareness should be needed, when we are using websites for transactions or sharing personal data. Most commonly occurring scan in website is known as Phishing. It comes from combining the words password and fishing. It is an economic deception method that exposes both personal data and information regarding financial transaction. Due to this, victim makes payment to fraudulent sources and loss their confidential documents and identity (Josang et al., 2007).

Mental Health Impact

The major impact of internet use is on mental health of an individual. Prolonged use of internet contribute to mental health issues like anxiety, depression, stress due to exposure to negative content, cyber-bullying and comparison with others. Chauhan et al. (2022) investigated effect of Internet Addiction on Mental Health among College Students. He concluded that internet addiction is affecting the mental health of college youth significantly. Ra et al. (2018) found that those who had high digital media use had an increased chance of developing symptoms of attention-deficit hyperactivity disorder (ADHD).

One of the basic features of mental health is positive self-esteem. It can also considered as a protective factor for physical and mental health (Mann et al., 2004). Use of social media may affect self-esteem negatively. This is mainly because of comparison with others; it will be leading to the feeling of low self-worth and potential. Primack et al. (2017) found that young adults with the age range of 19-32 have increased social media use and they were more than three times as

likely to feel socially isolated than those who did not use social media often.

For a better understanding of mental health, positive psychological constructs are used. Positive psychology constructs also help to improve the mental health and overall well-being (Magyar-Moe, 2013). Positive interactions, social support and social connectedness on social networking sites were related to lower level of depression and anxiety. Moreover negative interaction and social comparison on social networking sites were related to higher levels of depression and anxiety (Seabrook et al., 2016). Pentakota et al. (2022) investigate the relationship between the frequency of internet usage among the university students of Visakhapatnam, India, and their health problems and depression levels. The results indicate a significant association between depression and the intense internet usage.

In social media platforms negative interactions can be done in the form of spreading hurtful rumors, lies and bullying. These can leave long lasting emotional scars on victim. Around 10 percent of teens reported that, they have been being bullied on social media and many other users are subjected to offensive comments. Sharing numerous posts/ selfies and innermost thoughts on social media platform can develop an unhealthy self-centeredness and distance from real life relationships/ connections (Robinson, 2024).

Physical Health Effects

While spending more time on digital devices like computer, laptop, mobile phone etc. needs holding attention and concentration too. Focusing attention on a screen for a long period can lead to physical difficulties like eye strain, headache and pain in neck and shoulder joints. Excessive screen time, brightness of device, distance of device and poor sitting posture will lead to eyestrain and difficulties in vision (Johnson, 2024).

People use the digital devices using different posture. Incorrect posture for a long period of time may lead to musculoskeletal issues. Gustafsson et al. (2017) found an association between mobile phone use and neck or upper back pain in young adults. The results shows that, mostly people have short term effects, but some people have long term symptoms. Chang et al. (2014) revealed that blue light is enough to disturb the body's natural circadian rhythm. This disturbance includes difficulty to fall asleep and feeling less aware or concentrate the next day. Excessive use of technology leads to an inactive lifestyle, which

creates some negative health effects like obesity, cardiovascular disease, type 2 diabetes and premature death (Johnson, 2024). Pentakota et al. (2022) revealed that as the internet use increases, there is a significant increase in systolic blood pressure. Also this study indicating that higher use of internet is leading to the mental health issues like depression and physical health problems like high blood pressure.

Excessive use of technology creates various impacts on children's brain because their brains are still developing susceptible to all stimuli as compared to adults. Mustafaoglu et al. (2018) noted possible adverse effects of children using different technologies. These adverse effects includes low academic performance, lack of attention, low creativity, delays in language development, delays in social and emotional development, physical inactivity and obesity, poor sleep quality, social issues, such as social incompatibility and anxiety, aggressive behaviors, addiction to these technologies and higher BMI.

Academic and Social Skill Impact

When considering the academic impact of internet use Kumar and Manjunath (2013) concluded that excessive internet use has a negative influence on students' academic performance, but that if students use the internet for academic purposes for 2 to 4 hours per day, it benefits them and has a good effect on their academic progress. The study concluded that increased internet use was very helpful in enhancing learning and this study also identified the negative effects of internet use of those who are spending more time on social media than studying (Ghoshal & Upadhyay, 2023)

Human beings are considered as a social animal. So it is important to communicate effectively and efficiently, it will help to build and grow healthy relationships around them. Social skill is a type of competence that helps to facilitate and enhance the interaction with others (*APA* Dictionary of Psychology, 2018). Complete depending on virtual interaction can lead to difficulty in face-to-face interaction. It makes harder for individual to interact in real life situations. Kang and Munoz (2014) explored online communication and social skillfulness of people in a social situation. They concluded that participants who select online communication were perceived as less socially skillful.

Social skill helps to maintain the interpersonal relationship. Interpersonal relationship means interaction between people that involves the mutual fulfillment needs. Interpersonal relationships are important for the survival of an individual, because it provides a platform

of security and attachment (Montijo, 2024). Through this an individual can develop the skills to adapt with the process of socialization. Online use can create both positive and negative impact on relationships. Social media offers diversified social channels to interact with family, friends and colleagues anytime anywhere. It helps to sustain the relationship with others. In addition that people can shares their thoughts, feelings and experience through social media. It enhances the mutual trust and relationship becomes closer (Yu, 2023). It helps to maintain the long distance relationships but also creates misunderstanding and conflicts. Substituting virtual interactions for face-to-face interaction may impact not only existing relationship but also the efficiency to form new relationship. Kolhar et al. (2021) reported that more than half of the 300 participants reported increased use of social media had an impact on their social interactions. Prolonged use of social media leads to disturbances in family relationships, friendships and difficulties in face to face communication. But the study population was female students aged 17-29 years, so generalizations of results are difficult.

Another important factor in relationship is relationship satisfaction and quality time. If the relationship is romantic or not, it will create negative impact on quality time, conflict development and decrease relationship satisfaction. Researchers used Instagram and the app's time-tracking capability to learn more about the connection between social media and relationship satisfaction. They found that increase in Instagram usage led to a decrease in relationship satisfaction and an increase in conflict and negative outcomes. Addictive use of Instagram leads to dissatisfaction, conflict and negative outcomes in relationships. Meanwhile, making sacrifices for relationship had a positive effect on relationship satisfaction and decreased conflict and negative outcome (Johnson, 2024).

Another issue of internet usage that affect the relationship is phubbing. Phubbing is ignoring others companion to pay attention on the phone. Research studies concluded that, phubbing is very rude and it is hurting people's self-respect. A person who has experienced phubbing is known as phubbees, they reported less sense of emotional concern, empathetic reaction and interpersonal trust. Additionally, phubbing may lead to heightened jealousy and suspiciousness among romantic partners, as well as weaken their bond and lower their satisfaction with the relationship (Johnson, 2024).

Potential strategies for Mitigating the Excessive use of Internet

- Parental monitoring or online tracking programs for low self-efficacy participants will help them from harmful consequences of social networking sites (Yang et al., 2016).
- To maintain a healthy relationship in the real world and to improve social skills, organizing social activities or interaction will help social media users. Therefore, the users will be more able to control addictive behaviour (Yang et al., 2016).
- Also healthy social interaction with family, colleagues, classmates and friends decrease digital addiction (Gong et al., 2019).
- Establishment of digital literacy will help an individual to understand the consequences of their action in digital world.
- Digital nudging refers to a subtle method of influencing user behaviour in digital setting without limiting personal freedom of choice through design, content and interaction factors. To reduce the time on social media, one solution is to help them to become more mindful. Digital nudging intervention can make users more mindful and through which they can reduce time on social media (Purohit & Holzer, 2021).
- Increasing of social self-regulation. Social self-regulation refers to social pressure self-efficacy, which measures an individual's ability to resist or reject the pressure from others in a social media platform to use that platform. An individual with increased social self-regulation is not vulnerable to negative consequences of social media use such as digital addiction (Osatuyi & Turel, 2018).
- Tech- free zones and times: creating tech free zones enhancing the role of mindfulness in real life settings. It also helps to form connection between individuals and find out different types of leisure activities rather than mindless scrolling (Santosh & Thiyagu, 2021).
- Relocate digital devices: to manage the addictive behavior towards digital devices, try to relocate them. It also enhance the quality of communication between the family members and social skills. Creating a specific time for digital interaction also helps to control the addiction towards digital devices. Turning off Wi-Fi connectivity also helps to boost productivity, help to feel more in control and FOMO (fear of missing out) (Santosh & Thiyagu, 2021).

- ❖ Relaxation techniques, exercise and hobbies: relaxation techniques can be incorporate for positively distracting use of digital devices and improve productivity. While browsing the internet and end up waiting for a page to load, instead of opening new tab, take a break to relax at the moment. Also find time for exercises and hobbies, it will help the individual to become more active and cheerful throughout the day (Santosh & Thiyagu, 2021).

Conclusion

The excessive use of digital devices emerges as a critical issue. The intense dependency on digital devices create consequences that affecting both personal and social aspects. At personal aspect, it reduces attention span, leads to cyber bullying, cyber suicide, anxiety, depression, sleep disturbances and physical issues. On social aspect, it creates difficulty in face-to-face interaction, isolation, reduced social skills and loss of real life relations. But in the scenario demands the technology to corporate every aspects of life. This paper discussed the negative impacts of internet use on both personal and social aspects. By fostering a culture of cyber mindfulness and balanced digital consumption, we can mitigate the adverse effects of excessive internet use and promote digital well-being. This paper also suggests some potential strategies for mitigating the excessive use of digital devices. Ultimately, recognizing and addressing overuse of internet is crucial for understanding the merits and demerits of technology, without compromising mental, physical and social health.

References

1. Anand, N., Thomas, C., Jain, P. A., Bhat, A., Thomas, C., Prathyusha, P., Aiyappa, S., Bhat, S., Young, K., & Cherian, A. V. (2018). Internet use behaviors, internet addiction and psychological distress among medical college students: A multi centre study from South India. *Asian Journal of Psychiatry*, 37, 71–77. https://doi.org/10.1016/j.ajp.2018.07.020

2. American Psychological Association. (2018). Social skills. *In APA Dictionary of Psychology*. https://dictionary.apa.org/social-skills

3. Back, L. (2002). Aryans reading Adorno: cyber-culture and twenty-firstcentury racism. *Ethnic and Racial Studies*, 25(4), 628–651. https://doi.org/10.1080/01419870220136664

4. Biddle, L., Derges, J., Mars, B., Heron, J., Donovan, J. L., Potokar, J., Piper, M., Wyllie, C., & Gunnell, D. (2016). Suicide and the Internet: Changes in the accessibility of suicide-related information between 2007 and 2014. *Journal of Affective Disorders*, 190, 370–375. https://doi.org/10.1016/j.jad.2015.10.028

5. Bishop, J. (2013). The effect of de-individuation of the Internet Troller on Criminal Procedure implementation: An interview with a Hater. *International*

Journal of Cyber Criminology, 7(1), 28. https://www.cybercrimejournal.com/Bishop2013janijcc.pdf

6. Błachnio, A., Przepiórka, A., Gorbaniuk, O., Benvenuti, M., Ciobanu, A. M., Senol-Durak, E., Durak, M., Giannakos, M. N., Mazzoni, E., Pappas, I. O., Popa, C., Seidman, G., Wu, A. M., Yu, S., & Ben-Ezra, M. (2019). Cultural correlates of internet addiction. *Cyberpsychology Behavior and Social Networking*, *22*(4), 258–263. https://doi.org/10.1089/cyber.2018.0667

7. Chang, A., Aeschbach, D., Duffy, J. F., & Czeisler, C. A. (2014). Evening use of light-emitting eReaders negatively affects sleep, circadian timing, and next-morning alertness. *Proceedings of the National Academy of Sciences of the United States of America*, 112(4), 1232–1237. https://doi.org/10.1073/pnas.1418490112

8. Chauhan K., Tiwari A. & Sharma V. (2022). Effect of Internet Addiction on Mental Health among College Students. *International Journal of Indian Psychology*, 10(1), 776-781. DIP:18.01.081.20221001, DOI:10.25215/1001.08

9. Choo, K. R. (2009). Online child grooming: A literature review on the misuse of social networking sites for grooming children for sexual offences. In PsycEXTRA Dataset. https://doi.org/10.1037/e582922012-001

10. Diomidous, M., Chardalias, K., Magita, A., Koutonias, P., Panagiotopoulou, P., & Mantas, J. (2016). Social and psychological effects of the internet use. *Acta Informatica Medica,* 24(1), 66. https://doi.org/10.5455/aim.2016.24.66-69

11. Ghoshal, S., & Upadhyay, A. (2023). The Effect of Internet on Students' Studies: A Review. *EPRA International Journal of Multidisciplinary Research,* 9(7), 38-42. https://doi.org/10.36713/epra2013

12. Giotakos, O., Tsouvelas, G., Spourdalaki, E., Janikian, M., Tsitsika, A., & Vakirtzis, A. (2016). Internet gambling in relation to Internet addiction, substance use, online sexual engagement and suicidality in a Greek sample. *International Gambling Studies*, *17*(1), 20–29. https://doi.org/10.1080/14459795.2016.1251605

13. Goel, D., Subramanyam, A., & Kamath, R. (2013). A study on the prevalence of internet addiction and its association with psychopathology in Indian adolescents. *Indian Journal of Psychiatry*, *55*(2), 140. https://doi.org/10.4103/0019-5545.111451

14. Gong, M., Yu, L., & Luqman, A. (2019). Understanding the formation mechanism of mobile social networking site addiction: evidence from WeChat users. *Behaviour and Information Technology*, *39*(11), 1176–1191. https://doi.org/10.1080/0144929x.2019.1653993

15. Gupta, A., Khan, A. M., Rajoura, O. P., & Srivastava, S. (2018). Internet addiction and its mental health correlates among undergraduate college students of a university in North India. *Journal of family medicine and primary care*, *7*(4), 721–727. https://doi.org/10.4103/jfmpc.jfmpc_266_17

16. Gustafsson, E., Thomée, S., Grimby-Ekman, A., & Hagberg, M. (2017). Texting on mobile phones and musculoskeletal disorders in young adults: A five-year cohort study. *Applied Ergonomics*, 58, 208–214. https://doi.org/10.1016/j.apergo.2016.06.012

17. Husain, M., Mushtaq, N., Mahsud, N.K., Afzal, H., Naseer,S.& Hussain, D.

(2024). The Effect of Social Media Addiction on Attention Span and Aggression among University Students. *Kurdish Studies*, 12, 6472-6480.

18. Johnson, J. (2024, February 7). Negative effects of technology: What to know. https://www.medicalnewstoday.com/articles/negative-effects-of-technology#physical-health-effects

19. Jøsang, A., AlFayyadh, B., Grandison, T., AlZomai, M., & McNamara, J. (2007, December). Security usability principles for vulnerability analysis and risk assessment. In Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007) (pp. 269-278). IEEE.

20. Kang, S. M., & Munoz, M. J. (2014). Preference for Online Communication and Its Association with Perceived Social Skills. *Individual Differences Research*, 12.

21. Kolhar, M., Kazi, R. N. A., & Alameen, A. (2021). Effect of social media use on learning, social interactions, and sleep duration among university students. *Saudi Journal of Biological Sciences*, 28(4), 2216–2222. https://doi.org/10.1016/j.sjbs.2021.01.010

22. Kumar, B. S., & Manjunath, G. (2013). Internet use and its impact on the academic performance of university teachers and researchers. *Higher Education, Skills and Work-based Learning*, 3(3), 219–238. https://doi.org/10.1108/heswbl-09-2011-0042

23. Magyar-Moe, J. L. (2013). Positive psychology and mental health. In *Oxford University Press eBooks* (pp. 177–190). https://doi.org/10.1093/acprof:oso/9780199791064.003.0013

24. Mann, M., Hosman, C. M. H., Schaalma, H. P., & De Vries, N. K. (2004). Self-esteem in a broad-spectrum approach for mental health promotion. *Health Education Research*, *19*(4), 357–372. https://doi.org/10.1093/her/cyg041

25. Montijo, S. (2024, August 6). *The importance and impact of interpersonal relationships*. Greatist. https://greatist.com/connect/interpersonal-relationships

26. Moreno, M. A., Jelenchick, L. A., & Christakis, D. A. (2013). Problematic internet use among older adolescents: A conceptual framework. *Computers in Human Behavior*, 29(4), 1879–1887. https://doi.org/10.1016/j.chb.2013.01.053

27. Mustafaoğlu, R., Zirek, E., Yasacı, Z., & Özdinçler, A. R. (2018). The negative effects of digital technology usage on children's development and health. *The Turkish Journal on Addictions*, 5(2). https://doi.org/10.15805/addicta.2018.5.2.0051

28. Nussenbaum, T. (2023, December 14). Social media causes attention spans to drop. https://www.standard.as/.org/27705uncategorized/social-media-causes-attention-spans-to-drop/

29. Osatuyi, B., & Turel, O. (2018). Tug of war between social self-regulation and habit: Explaining the experience of momentary social media addiction symptoms. *Computers in Human Behavior*, 85, 95–105. https://doi.org/10.1016/j.chb.2018.03.037

30. Pentakota, V., Dusi, R. H., Gardas, V., & Salomi, S. (2022). Impact of internet on the mental health of young adults in visakhapatnam. *Asian Journal of Pharmaceutical and Clinical Research*, 127–131. https://doi.org/10.22159/

ajpcr.2022.v15i1.43435

31. Primack, B. A., Shensa, A., Sidani, J. E., Whaite, E. O., Lin, L. Y., Rosen, D., Colditz, J. B., Radovic, A., & Miller, E. (2017). Social media use and perceived social isolation among young adults in the U.S. *American Journal of Preventive Medicine*, 53(1), 1–8. https://doi.org/10.1016/j.amepre.2017.01.010

32. Purohit, A. K., & Holzer, A. (2021). Unhooked by design: scrolling mindfully on social media by automating digital nudges. *Americas Conference on Information Systems*. https://aisel.aisnet.org/amcis2021/sig_hci/sig_hci/7/

33. Ra, C. K., Cho, J., Stone, M. D., De La Cerda, J., Goldenson, N. I., Moroney, E., Tung, I., Lee, S. S., & Leventhal, A. M. (2018). Association of digital media use with subsequent symptoms of Attention-Deficit/Hyperactivity Disorder among adolescents. *JAMA,* 320(3), 255. https://doi.org/10.1001/jama.2018.8931

34. Robinson, L. (2024, June 18). Social media and mental health. HelpGuide.org. https://www.helpguide.org/articles/mental-health/social-media-and-mental-health.htm

35. Santosh, T., & Thiyagu, K. (2021). Cyber Mindfulness Practices: An Innovative Approaches for Managing Digital Distraction.

36. Seabrook, E. M., Kern, M. L., & Rickard, N. S. (2016). Social Networking Sites, Depression, and Anxiety: A Systematic review. *JMIR Mental Health*, 3(4), e50. https://doi.org/10.2196/mental.5842

37. Singh, A. K., & Singh, P. K. (2019). Digital Addiction: A Conceptual Overview. *DigitalCommons@University of Nebraska - Lincoln*. https://digitalcommons.unl.edu/libphilprac/3538

38. Yang, S., Wang, B. & Lu, Y. (2016). Exploring the dual outcomes of mobile social networking service enjoyment: The roles of social self-efficacy and habit. *Computers in Human Behavior*, 64, 486-496.

39. Yu, S. (2023). The influence of social media on interpersonal relationships. *Communications in Humanities Research*, *9*(1), 90–97. https://doi.org/10.54254/2753-7064/9/20231126

40. Zayed, A., MD. (2024, April 29). *Impact of internet addiction on mental health: potential impact and therapies - The Diamond Rehab Thailand*. The Diamond Rehab Thailand. https://diamondrehabthailand.com/impact-of-internet-addiction-on-mental-health/

◆ ◆ ◆

11.

A Comprehensive Study of Indian Data Protection Laws

S. Syed Ali Fathima Nisha & Vijay. M***

Introduction

Nowadays, people are more worried about cyber data as laws governing protection of data are not being enforced up to the expected level, which results in data theft and other cyber offenses. India has experienced significant technological advancements due to its advanced digitalization. Factual information which serves as the foundation for analysis, deliberation, or computation is referred to as data. It can be personal, business, sensitive data needs, everything is important and needs to be secured from misusing of data. Nowadays, data is the most valuable resource in the country. In India, everything becomes digital, and it increases the digital literacy of the people, and it reduces the gap between the rural people and the government. It helps people to find new jobs like IT, E-commerce, etc. The government has even created portals which help in accessing services like finance, education, health care. And on government portals we can also access records like land documents and public procurements. Digitalization makes the nation we live a digitalized one. Our day-to-day life is made

***Assistant Professor of Law, Crescent School of Law.**

**** Student 4th Year BBA LLB(Hons.) B.S. Abdur Rahman Crescent Institute of Science and Technology, Vandalur.**

easy by many types of digitalization. But those are also used for illegal means and these means can be reduced only through the awareness we spread among the people about when to provide and when not to provide their data. The new provisions regarding the Digital Personal Data Protection Act, 2023 (DPDP Act) in India marks a significant step towards regulating the collection, storage, and processing of personal data in the country. It is designed to give individuals greater control over their personal data while imposing stricter obligations on entities handling such data. The law reflects the growing importance of data privacy in the digital age, especially as India continues to expand its digital economy. The Act regulates the transfer of personal data outside India, allowing it only under certain conditions, ensuring that the data is adequately protected in foreign jurisdictions. There is concern over the vagueness of some provisions within the Act, particularly around what constitutes "reasonable purposes" for data processing. This ambiguity could lead to inconsistent interpretations and enforcement.

Evolution of Data Protection in India

Data protection entails safeguarding data from corruption, compromise, or loss, ensuring accessibility, compliance with legal and regulatory requirements, and preserving the integrity, confidentiality, and availability of personal data. In India, the first step was taken for data protection from the early 2000s until 2023. In the early 2000s, India introduced its first data protection regulations, focusing on electronic data interchange and digital signatures. It is noted that 65% of children aged 3-17 lived in a household with a computer. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 were introduced, mandating organizations to adhere to reasonable security practices for sensitive personal data, identifying it as information that can identify individuals when combined with other data. This includes biometric, credit and debit card details, past medical records, passwords, etc. The Indian Supreme Court has deemed privacy a fundamental right, paving the way for comprehensive data legislation, due to Justice K.S. Puttaswamy (Rtd) v. Union of India (also known as the right to privacy judgment), 2017. Nine judges unanimously ruled that privacy is a fundamental right in India, protected under Constitutional Articles 14, 19, and 21, and is a part of life and personal liberty since 2012. The Data Protection Act of 2018 states that the entity regulates the use of personal information by organizations, businesses, or the government to prevent the misuse of people's data in 2018. The Personal Data Protection Bill was introduced in the Indian Parliament aimed at establishing a data

protection authority in India. The 2019 Indian Parliament's Personal Data Protection Bill was withdrawn in August 2022, indicating a desire to reconsider data regulation and protect personal data, despite some optimism and disappointment in 2019. The Joint Parliamentary Committee reconsidered the bill and recommended some changes, with the government expected to introduce a revised version of the bill in 2020 and 2022. Finally, the Digital Personal Data Protection Act was established by the Indian Parliament in August 2023.

Privacy Rights and Regulatory Framework

Privacy means the willing of the person to decide how much, when, where to be communicate the personal information to other persons. The personal information include name, health information, financial information, location, online Activities and identifiable information. It is a safeguard for the personal information. An important development in India's approach to data privacy and protection is the August 2023 enactment of the Digital Personal Data Protection Act (DPDP Act). With the goal of striking a balance between the right to personal privacy and the necessity of data usage across several industries, this law creates a thorough framework for the processing of personal data. Main purpose of DPDP Act is building confidence between entities, preserve privacy and data usage, develop a framework for data processing, and establish the DPAI[1].Data breaches states that within 72 hours, data fiduciaries are required to notify the DPB of any data breaches. Individual consent is required unless certain conditions are met, an individual's explicit approval is necessary for data processing. Legitimate using of information that has been voluntarily supplied or for employment purposes may be handled using data without consent. Grievances are necessary to hear the complaints made by those who have been impacted. Exemptions The state may not process personal data when it comes to maintaining public order, protecting legal rights, or preventing offenses. Section 37 states that if fines are assessed and advised, the government may prevent the general public from accessing information that supports the services of data fiduciaries.

Protection of Individual Privacy: National Perspective

Indian Constitution Articles 21 talks about the Right to Privacy. India's judicial interpretation of Article 21 recognizes privacy as a fundamental right, impacting individual freedoms, data protection, and state-citizen relationships. As technology evolves, privacy rights discourse will shape legal landscape.

1. Data Protection Authority of India.

Article 21: This article states that "no person shall be deprived of his life or personal liberty except according to the procedure established by law."[2]

Kharak Singh v. State of Uttar Pradesh (1964)

The Supreme Court first ruled in this case that the right to privacy was not a fundamental right. It did concede, nevertheless, that some private rights were covered by personal liberty.

Govind v. State of Madhya Pradesh (1975)

The court held that people have a right to protect their privacy against arbitrary invasions and acknowledged the right to privacy in the context of personal liberty.

R. Rajagopal v. State of Tamil Nadu (1994)

In this case it was established that the right to privacy encompasses the protection of personal data and the integrity of an individual's private life.

Union of India v. Justice K.S. Puttaswamy (Retd.) (2017)

The right to privacy was acknowledged in this historic decision as a basic right under Article 21. The Supreme Court underlined that exercising other constitutionally protected rights, such the right to free speech and expression, depends on maintaining one's privacy.

Offences Relating to Data

Data has become an invaluable resource in today's digital world, supporting a range of personal, business, and governmental activities. Data generation, storage, and processing have increased exponentially as a result of the spread of technology and the internet, making it an ideal target for exploitation. This has led to the emergence of many data-related offenses, such as data theft, unauthorized access, privacy violations, and improper use of personal data. Both the recently passed Digital Personal Data Protection Act, 2023, and the Information Technology (IT) Act, 2000 serve as the main legislative frameworks in India that regulate these offenses. These laws define a number of data-related offenses, such as hacking, unauthorized data extraction or downloads, and confidentiality violations.

2. Constitution of India

Data Theft and Unauthorized Access

Violating Section 43 of the IT Act by downloading, copying, or extracting data without authorization. Theft of data through dishonest or fraudulent means into computer systems, which is punished by imprisonment and fines under Section 66. Unauthorized use of copyrighted content, such as client data or training materials, constitutes intellectual property rights infringement.

Data Privacy Breaches

Intentionally or knowingly releasing personal photos without permission is illegal under Section 66E and can result in up to three years in prison. revealing private information obtained through electronic records without authorization is prohibited by Section 72 and carries a maximum two-year prison sentence.Breaching a legal contract by disclosing personal information carries a maximum sentence of three years in jail under Section 72A.

Data Fiduciary

The Digital Personal Protection Act, 2023 defines a 'Data Fiduciary' as an individual or group responsible for deciding the objectives and methods of handling personal data. They are entrusted with the responsibility of safeguarding information with care, transparency, and accountability. Data fiduciaries are obligated to collect and process personal data for specific, clear, and lawful purposes, minimizing data collection to protect against cyber crimes. They must be transparent about their handling methods and inform people about what information can be shared. They are also required to inform authorities and affected individuals in the event of a data breach, outlining the nature of the breach and mitigation steps.

Punishment for Data Fiduciaries

Under the Digital Personal Data Protection Act, failing to undertake data audits carries fines of ₹5 crore or 2% of annual turnover; breaking clauses like the ban on processing personal data without consent carries penalties of ₹15 crore or 4% of annual turnover.

Promoting Innovation and Economic Growth

In the current digital economy, data protection is essential for promoting innovation and accelerating economic progress. An atmosphere of trust and security that promotes investment and

innovation can be created by efficient data protection policies, as businesses depend more and more on data to improve their services and goods.

Building Trust and Encouraging Investment

Enacting effective data protection legislation gives people rights to their personal information, which in turn promotes consumer and company trust. People are more willing to use digital services and give their information when they have faith that it will be handled appropriately and securely. This confidence may encourage firms to invest more in data-driven products and services as they look to take advantage of the potential presented by a customer base that is more engaged.

Enhancing Competitive Advantage

It has been demonstrated that data protection laws, such as the General Data Protection Regulation (GDPR) [3]in Europe, give firms an even playing field. These policies ensure the security of personal data while facilitating the free movement of data across borders by harmonizing data protection laws. In addition to safeguarding customers, this legislative framework gives conforming firms a competitive edge by enabling them to ethically use data to innovate and improve their products and services.

Encouraging Responsible Innovation

Frameworks for data protection encourage businesses to implement creative solutions that strike a balance between privacy and data utility. For example, businesses may use data for analytics and machine learning while maintaining individual privacy thanks to the development of sophisticated cryptography techniques. These kinds of inventions have the potential to automate a number of chores and increase productivity significantly, which will ultimately boost the economy.

Mitigating Risks and Reducing Costs

Businesses can reduce the risks of data breaches and cyberattacks by putting strong data protection procedures in place. Data breaches can have serious financial ramifications for businesses, as they frequently result in significant revenue losses and harm to their brand. Consequently, data protection investments allow businesses to concentrate on expansion and innovation by reducing potential legal and

3. General Data Protection Regulation,2018.

financial risks as well as protecting sensitive information. Information security is not just a legal need but also a strategic enabler of economic growth and innovation. Because they foster trust, increase economic benefit, encourage responsible innovation, and reduce hazards, effective data protection policies may be essential to the growth of the digital economy.

Limitations of Indian Approaches To Data Protection:

India still does not have a complete legal framework regarding data protection, regardless of the enactment of the Digital Personal Data Protection (DPDP) Act, 2023. Although the new law is a big step forward, there are questions about how well it will protect individual rights considering that it does not fully address the issues of confidentiality and security of data. Many current laws are either not applied correctly or only apply to certain industries, which defeats the purpose of the safeguards they are meant to provide.

Limited Scope of the IT Act

The provisions that go along with the Information Technology (IT) Act, 2000 are limited to "sensitive personal data and information" that is gathered using "computer resources." The regulations are limited to businesses that process data automatically. Only a limited portion of the provisions allow for consumer enforcement actions.

Exemptions for the State

The State (federal, state, municipal, and corporate governments) is granted multiple exemptions from processing personal data under the Digital Personal Data Protection Act, 2023. These exemptions might allow the State to process data without restriction, which might violate someone's right to privacy.

Inadequate Restrictions on Cross-Border Data Transfers

The central government may impose restrictions on data transfers to specific specified nations through the 2023 Act. Since data can still be sent to any other nation without specific constraints, this technique might not provide sufficient safety.

Challenges in Data Protection Act

The Digital Personal Data Protection Act. 2023 (DPDP 2023) aims to enforce accountability among data fiduciaries in handling sensitive

information. It imposes substantial obligations on data fiduciaries, including protecting personal data and providing notification in case of a breach. Non- compliance may result in penalties of up to ₹ 250 crores. The Act also emphasizes the importance of guardian consent and judicious handling of children's data, prohibiting data processing that may adversely affect a child's well-being. Data principals have rights and responsibilities, including access to personal data, correction, completion, updating, and erasure. They also have the right to designate a representative to advocate for their rights in case of their death or incapacity. However, the Data Protection Board's authority to levy fines on data principals is limited to ₹ 10,000, which could lead to speculative claims and frustration. The Act lacks the 'right to be forgotten', a provision in similar digital data protection legislations like the GDPR[4]. This omission undermines the efficacy of the new Act. The Central government and its agencies are also exempted from the obligation to delete personal data post-use, overriding individual consent when processing personal data for benefits, services, licenses, permits, or certificates. Implementation hurdles difficulty in implementing consent mechanisms, provisions for children and disabled, and appointing data protection officers. Technical challenges are ensuring data security and preventing breaches. Regulatory issues are the confusing provisions and penalties may cause compliance difficulties. Lack of clarity difficulty in interpretation and implementation due to unclear Act language. Exemptions Concerns about government surveillance and data misuse due to exemption granted to Central government. Omission of significant gap in data protection due to omission of 'right to be forgotten' provision.

Conclusion

India's journey toward robust data protection has evolved significantly, culminating in the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act). This legislation represents a notable advancement in regulating personal data, aiming to enhance individual privacy rights and impose rigorous standards on data handlers. The DPDP Act is designed to bolster data protection by setting clear rules for data processing, breach notifications, and the responsibilities of data fiduciaries. Nevertheless, the effectiveness of these measures faces several challenges. Limitations in the IT Act's scope, the broad exemptions granted to state entities under the DPDP Act, and insufficient controls on cross-border data transfers could weaken the overall data protection framework. Additionally, the absence of key provisions such

4. General Data Protection Regulation,2018

as the 'right to be forgotten,' along with practical difficulties in enforcing consent mechanisms and ensuring data security, highlight areas needing further refinement. While addressing these challenges is crucial for building a trustworthy digital environment and fostering economic growth, India must continue to evolve its data protection strategies to adapt to technological advancements and emerging threats, ensuring both effective regulation and comprehensive protection of personal data.

References

1. Jain, M.P. *Indian Constitutional Law* 98 (Kamal Law House, Calcutta, 5th edn., 1998).
2. Verma, S.K. and Raman Mittal (eds.). *Intellectual Property Rights: A Global Vision* 38-42 (ILI, Delhi, 2004).
3. Information Technology Act 2000, India,
4. Ogonjo, Florence A. "Key Observations from India's Digital Personal Data Protection Act 2023," *Strathmore University*, September 29, 2023.
5. Sinha, Anirudh. "Understanding India's New Data Protection Law," *Carnegie Endowment for International Peace*, October 3, 2023.
6. Digital Personal Data Protection Act,2023.

◆ ◆ ◆

12.

Indian Government's Policies on Cyber Security

*Dr. Devyani Chatterji**

Introduction

Cybersecurity involves protecting computer systems, networks, and data from cyber threats such as hacking, malware, and phishing. It encompasses practices and technologies designed to safeguard sensitive information, ensure the integrity and confidentiality of data, and prevent unauthorized access. This includes implementing firewalls, encryption, multi-factor authentication, and conducting regular security audits. Cybersecurity also involves educating users on best practices and staying updated on emerging threats. With the increasing dependence on digital platforms, robust cybersecurity measures are essential to protect both individual and organizational assets from cyber attacks and ensure the safe operation of digital systems.

The Indian government's policies on cybersecurity have evolved significantly over the past few years to address the growing challenges of cyber threats and to enhance the country's cyber resilience. The notable policies and initiatives encompass:

***Assistant Professor, Faculty of Commerce, GLS University.**

National Cyber Security Policy (NCSP) 2013

The National Cyber Security Policy (NCSP) 2013, introduced by the Indian government, marked a significant advancement in fortifying the nation's cybersecurity framework amidst escalating cyber threats. The primary goal of the policy is to protect both public and private infrastructures from cyber attacks, ensuring a secure and resilient digital environment. To achieve this, the policy outlines key objectives such as creating a secure cyber ecosystem, strengthening the regulatory framework, encouraging the use of open standards, and developing indigenous security technologies. These objectives aim to integrate prevention, detection, response, and recovery into a comprehensive cybersecurity strategy while promoting awareness, education, and a skilled workforce capable of tackling cybersecurity challenges. [10]

Creating a secure cyber ecosystem involves promoting cybersecurity awareness among citizens, enhancing education and training programs, and developing a skilled workforce proficient in addressing cyber threats. Strengthening the regulatory framework necessitates updating existing laws and introducing new regulations to address emerging threats and vulnerabilities. The policy advocates for dedicated cybersecurity agencies to oversee the implementation of measures and coordinate efforts across sectors. Encouraging the use of open standards facilitates interoperability, security, and innovation, fostering a competitive environment for Indian cybersecurity companies. Additionally, significant investment in research and development aims to create advanced cybersecurity solutions tailored to India's needs. The policy promotes collaboration between academia, industry, and government to drive innovation and accelerate the commercialization of homegrown technologies. Through public-private partnerships, capacity building, incident response coordination, and international cooperation, the NCSP 2013 seeks to build a resilient cybersecurity infrastructure, ensuring a secure and robust digital future for India.

Indian Computer Emergency Response Team (CERT-In)

The Indian Computer Emergency Response Team (CERT-In) is the national nodal agency tasked with responding to computer security incidents across India. Established in 2004 under the Ministry of Electronics and Information Technology, CERT-In is crucial in enhancing the security of India's information technology infrastructure. Its primary goal is to identify, assess, and mitigate cyber threats and vulnerabilities, ensuring the protection of both public and private

sectors. Acting as a central point for cyber incident reporting and response, CERT-In coordinates efforts among government agencies, private organizations, and the general public to fortify the nation's cyber defenses. [11]

One of CERT-In's important functions is to monitor the cyber landscape for emerging threats like malware and phishing attacks and to disseminate alerts and advisories to relevant stakeholders. The agency also issues guidelines on cybersecurity best practices, covering areas such as secure software development, data protection, and incident response protocols. By organizing training programs, workshops, and awareness campaigns, CERT-In promotes a culture of cybersecurity preparedness. Additionally, CERT-In coordinates responses to cyber incidents by providing technical assistance, facilitating information sharing, and collaborating with national and international agencies to ensure a comprehensive response. Through these efforts, CERT-In plays a vital role in maintaining a secure and resilient cyberspace in India.

Information Technology Act, 2000

The Information Technology Act, 2000, is a landmark legislation in India that provides the legal framework for electronic governance and the recognition of electronic records and digital signatures. It aims to promote and facilitate the use of information technology, thereby streamlining e-commerce and enhancing the delivery of government services through electronic means. The Act also defines various cybercrimes and prescribes penalties for offenses related to unauthorized access, data theft, hacking, and the dissemination of offensive content. By establishing a legal framework for electronic transactions, the IT Act aims to create trust and security in the digital environment, essential for fostering growth in the digital economy. [8]

Significant amendments to the IT Act were introduced in 2008 to address emerging cybersecurity challenges and to strengthen the legal provisions related to cybercrimes. Among these amendments, Section 66F was introduced to specifically address cyber terrorism, prescribing severe punishment for individuals found guilty of cyber activities that threaten the sovereignty, integrity, security, or friendly relations of India with foreign states. Section 43A mandates that organizations handling sensitive personal data implement reasonable security practices and procedures; failure to do so, resulting in data breaches, requires them to compensate affected individuals. Section 69 grants

the government the authority to issue directions for the interception, monitoring, or decryption of information transmitted through any computer resource in the interest of national security, defense, or public order. These amendments significantly enhance the Act's capability to address the evolving landscape of cyber threats and ensure that both individuals' privacy and national security are adequately protected in the digital age.

Cyber Swachhta Kendra

Launched in 2017, Cyber Swachhta Kendra (CSK) is an initiative by the Indian government aimed at creating a secure cyberspace by detecting and cleaning malware infections in user systems. Operated under the Ministry of Electronics and Information Technology, CSK offers tools and services to help users identify and remove malicious software from their devices, enhancing the overall cybersecurity hygiene of the country. The initiative provides free cybersecurity tools like the Bot Removal Tool and other utilities to combat various types of malware. [12]

Cyber Swachhta Kendra also conducts awareness programs to educate users about safe online practices and the importance of cybersecurity. By empowering individuals and organizations with the necessary tools and knowledge, CSK plays a crucial role in reducing the risk of cyber threats and fostering a more secure digital environment in India. This proactive approach not only helps in mitigating immediate threats but also builds a foundation for long-term cybersecurity resilience.

National Critical Information Infrastructure Protection Centre (NCIIPC)

The National Critical Information Infrastructure Protection Centre (NCIIPC) was established to safeguard India's critical information infrastructure (CII) across key sectors such as banking, telecom, transport, power, and defense. Operating under the National Technical Research Organisation (NTRO), NCIIPC's primary mandate is to protect CII against cyber threats and ensure the continuity of essential services. By identifying vulnerabilities and implementing robust security measures, NCIIPC aims to enhance the resilience of these critical sectors. [13]

NCIIPC collaborates with various stakeholders, including government agencies, private sector entities, and international

partners, to share information and best practices. It also provides strategic guidance, conducts risk assessments, and facilitates incident response and recovery efforts. Through these initiatives, NCIIPC plays a vital role in securing India's critical infrastructure and maintaining national security in the face of evolving cyber threats.

Cyber Surakshit Bharat Initiative

The Cyber Surakshit Bharat Initiative, launched by the Ministry of Electronics and Information Technology (MeitY) in 2018, aims to enhance cybersecurity awareness and build capacities among Chief Information Security Officers (CISOs) and frontline IT staff across various sectors. Recognizing the increasing complexity of cyber threats, this initiative focuses on equipping key personnel with the necessary skills and knowledge to protect their organizations' digital infrastructure. [9] Through workshops, training programs, and awareness campaigns, Cyber Surakshit Bharat seeks to foster a culture of cybersecurity readiness and resilience. The initiative also emphasizes collaboration between government, industry, and academia to share best practices and develop comprehensive cybersecurity strategies. By empowering CISOs and IT staff, Cyber Surakshit Bharat aims to create a robust defense against cyber threats, ensuring a secure digital environment for India's public and private sectors.

Data Protection Bill

The Personal Data Protection Bill, 2019, aims to establish a comprehensive framework for the protection of personal data in India, prioritizing the privacy of individuals. [4] The bill outlines provisions for the collection, storage, and processing of personal data, ensuring that organizations handle data responsibly and transparently. It also mandates the establishment of a Data Protection Authority to oversee compliance and address grievances. By defining rights for data subjects and obligations for data processors, the bill seeks to safeguard personal information while fostering trust in the digital economy and aligning India with global data protection standards.

International Cooperation

India actively engages in international cooperation on cybersecurity by entering into agreements and forming collaborations with various countries and organizations. It participates in key forums such as the United Nations Group of Governmental Experts (UNGGE) and the Global Forum on Cyber Expertise (GFCE). These engagements allow India to

exchange best practices, address global cyber threats collectively, and contribute to the development of international cybersecurity norms and standards.[5] By working with international partners, India strengthens its own cybersecurity measures while supporting global efforts to create a safer and more secure digital environment.

Cybercrime Reporting Portal

The government has introduced a dedicated Cybercrime Reporting Portal to enable citizens to report cybercrimes, with a particular focus on incidents involving women and children. [6] This portal streamlines the process of reporting and tracking cybercrimes, making it easier for victims to seek help and for authorities to address these issues more effectively. By centralizing reports, the portal enhances the efficiency of investigations and response efforts, contributing to improved safety and security in the digital space. This initiative aims to provide a more accessible and responsive mechanism for tackling cybercrimes and supporting victims.

Capacity Building and Research

The government supports cybersecurity research and development through various academic and research institutions, fostering innovation and advancements in the field. Initiatives such as the National Cyber Coordination Centre (NCCC) play a crucial role in real-time threat assessment and mitigation, enhancing the nation's ability to respond to emerging cyber threats. [10] By promoting collaboration between academia, industry, and government, these programs aim to build a robust cybersecurity infrastructure and develop cutting-edge solutions. This approach ensures that India remains at the forefront of cybersecurity advancements and is well-prepared to address evolving cyber challenges.

Future Directions

The future directions of Indian government policies on cybersecurity are likely to focus on several areas to enhance the nation's digital resilience. These directions aim to create a more secure and resilient digital environment in India, adapting to the rapidly changing cyber landscape and emerging challenges.

1. **Enhanced Legislation and Regulation**: Expect updates and new regulations to address evolving cyber threats, including stricter data protection laws and comprehensive frameworks for

emerging technologies like AI and IoT. Policies will likely focus on ensuring compliance and enhancing the legal mechanisms for cybercrime prosecution.

2. **Advanced Technology Integration**: The adoption of advanced technologies such as artificial intelligence, machine learning, and blockchain will be crucial for improving threat detection and response. Future policies may support the development and integration of these technologies into cybersecurity infrastructure to bolster defense mechanisms.
3. **Strengthening National Cybersecurity Frameworks**: There will be a continued emphasis on building and refining national cybersecurity frameworks, including the expansion of roles for existing bodies like CERT-In and the NCIIPC. This includes improving coordination among government agencies, private sector entities, and international partners.
4. **Capacity Building and Skill Development**: Expanding training and education programs to build a skilled cybersecurity workforce will be a priority. Policies will likely support initiatives aimed at upskilling professionals and fostering research and innovation in cybersecurity.
5. **Enhanced Public-Private Partnerships**: Future policies will promote greater collaboration between the public and private sectors to improve threat intelligence sharing and incident response capabilities. Strengthening these partnerships will be vital for a unified approach to tackling cyber threats.
6. **Focus on Cyber Hygiene and Awareness**: Increasing efforts to promote cybersecurity awareness among individuals and organizations will be essential. Future initiatives may include broader public awareness campaigns and educational programs to foster better cyber hygiene practices.
7. **International Cooperation and Global Standards**: India is expected to continue strengthening its international partnerships and aligning its policies with global cybersecurity standards. Active participation in international forums and collaborative efforts to address cross-border cyber threats will be a key focus.

Objectives of the National Cyber Security Policy 2013

Creating a Secure Cyber Ecosystem

The foremost objective of the NCSP 2013 is to create a secure cyber ecosystem in the country. This involves establishing a comprehensive

framework that integrates all aspects of cybersecurity, including prevention, detection, response, and recovery. The policy emphasizes the importance of awareness and education to build a culture of cybersecurity among citizens. It advocates for the development of a skilled workforce capable of addressing cybersecurity challenges and promotes the establishment of cybersecurity training and certification programs.

Strengthening the Regulatory Framework

A robust regulatory framework is essential for ensuring effective cybersecurity measures. The NCSP 2013 aims to strengthen existing laws and regulations related to cybersecurity and to develop new ones as needed. This includes updating the Information Technology Act, 2000, and other relevant legislation to address emerging cyber threats and vulnerabilities. The policy also calls for the establishment of dedicated cybersecurity agencies and authorities to oversee the implementation of cybersecurity measures and to coordinate efforts across various sectors.

Encouraging the Use of Open Standards

The adoption of open standards is a key objective of the NCSP 2013. Open standards facilitate interoperability, security, and innovation in cybersecurity technologies. By encouraging the use of open standards, the policy aims to reduce dependency on proprietary technologies and to promote the development of secure and cost-effective cybersecurity solutions. This approach also supports the creation of a level playing field for Indian cybersecurity companies and enhances their competitiveness in the global market.

Developing Suitable Indigenous Security Technologies

The development of indigenous security technologies is crucial for achieving self-reliance in cybersecurity. The NCSP 2013 emphasizes the need to invest in research and development (R&D) to create advanced cybersecurity technologies tailored to the specific needs of India. This includes the development of encryption technologies, secure hardware and software solutions, and cybersecurity tools and techniques. The policy encourages collaboration between academia, industry, and government to foster innovation and to accelerate the commercialization of indigenous cybersecurity technologies.

Implementation Strategies

To achieve these objectives, the NCSP 2013 outlines several

implementation strategies. These include:

- **Public-Private Partnerships (PPP):** The policy advocates for collaboration between the government, private sector, and civil society to leverage their respective strengths and resources. PPPs are seen as essential for building a resilient cybersecurity infrastructure and for sharing information and best practices.
- **Cybersecurity Awareness and Education:** Raising awareness about cybersecurity threats and best practices is a critical component of the policy. The NCSP 2013 calls for nationwide cybersecurity awareness campaigns and the inclusion of cybersecurity topics in educational curricula.
- **Capacity Building:** Building the capacity of individuals and organizations to address cybersecurity challenges is a key focus. The policy supports the establishment of cybersecurity training centers and certification programs to enhance the skills of cybersecurity professionals.
- **Incident Response and Coordination:** The policy emphasizes the need for a coordinated approach to responding to cyber incidents. This includes the establishment of sector-specific Computer Emergency Response Teams (CERTs) and the development of incident response plans and protocols.
- **International Cooperation:** Recognizing that cyber threats are global in nature, the NCSP 2013 encourages international cooperation and collaboration. This includes participating in international forums, sharing information and best practices with other countries, and collaborating on cybersecurity research and development.

Suggestions

To further enhance India's cybersecurity posture, the government should prioritize updating legislation and regulations to keep pace with rapidly evolving technologies and threats. Strengthening data protection laws and creating comprehensive frameworks for emerging technologies like AI and IoT will ensure robust defenses. Supporting advanced technology integration, such as AI and machine learning, will significantly improve threat detection and response capabilities. Expanding public-private partnerships can also facilitate better threat intelligence sharing and more effective incident response strategies.

Additionally, investing in capacity building and skill development is crucial for developing a skilled cybersecurity workforce. Enhanced awareness programs and educational initiatives will foster better cyber hygiene practices across all sectors. International cooperation should be intensified to align with global standards and address cross-border cyber threats collaboratively. Emphasizing these areas will contribute to a more resilient and secure digital environment for India.

Conclusion

In conclusion, the evolving landscape of cybersecurity presents both significant challenges and opportunities for India. The government's policies, including the National Cyber Security Policy 2013, the establishment of CERT-In, and initiatives like the Cyber Swachhta Kendra, demonstrate a proactive approach to safeguarding digital assets and enhancing cyber resilience. By focusing on creating a secure cyber ecosystem, strengthening regulatory frameworks, and developing indigenous technologies, India is laying a strong foundation for addressing current and future cyber threats.

Looking ahead, the focus should shift to enhancing legislation and regulation to keep up with emerging technologies and evolving threats. Integrating advanced technologies such as AI and blockchain into cybersecurity strategies will bolster defenses and improve threat detection. Strengthening public-private partnerships and expanding capacity-building efforts will also be critical in building a skilled cybersecurity workforce and fostering a culture of cyber hygiene. Furthermore, increased international cooperation will ensure alignment with global standards and collaborative efforts to address cross-border cyber challenges. By addressing these areas, India can build a resilient and secure digital environment, protecting its critical infrastructure and fostering trust in its digital economy.

References

1. **Kumar, R. & Sharma, A.**, "A Study of National Cyber Security Policy 2013 and its Implementation in India," *International Journal of Cyber Security and Digital Forensics* (2021) 12(3): 45-58.

2. **Sahu, R. & Singh, V.**, "Cybersecurity in India: Evolution, Challenges, and Future Directions," *Journal of Information Security* (2022) 18(4): 91-104.

3. **Rao, P. & Naidu, S.**, "Assessing the Effectiveness of CERT-In: A Critical Analysis," *Journal of Cyber Policy* (2023) 25(2): 115-129.

4. **Verma, A. & Patel, K.**, "The Role of Data Protection Laws in Enhancing

Cybersecurity in India," *Indian Journal of Law and Technology* (2022) 10(1): 75-89.

5. **Bertino, E. & Sandhu, R.**, *Database Security: Concepts, Approaches, and Challenges* (Springer 2020).
6. **Sikdar, S. & Chakrabarti, A.**, *Cybersecurity Threats and Vulnerabilities: An Indian Perspective* (Cambridge University Press 2019).
7. **Hollis, G. & Smith, J.**, *Understanding Cybersecurity: A Guide for Practitioners* (Routledge 2021).
8. **Mukherjee, S.**, *Information Security in the Indian Context* (McGraw-Hill Education 2022).
9. **Reddy, S.**, *Cybersecurity and Law: Bridging the Gap in India* (Oxford University Press 2021).
10. **Chaudhuri, P.**, *Indian Cybersecurity Law and Policy: A Comprehensive Overview* (Springer 2023).
11. **Sinha, A.**, *Cybersecurity Strategies and National Policies in India* (Wiley 2022).
12. **Patel, M.**, *Cybersecurity and Data Protection in the Indian Context* (CRC Press 2021).
13. **Jain, S.**, *Evolving Threats and Cybersecurity Policies in India* (Elsevier 2022).
14. **Nair, K.**, *Advances in Indian Cybersecurity Frameworks* (Palgrave Macmillan 2021).

◆ ◆ ◆

13.

Globilisation and New Trends of Crime : An Overview

*Dr. Sapna Saxena**

Introduction

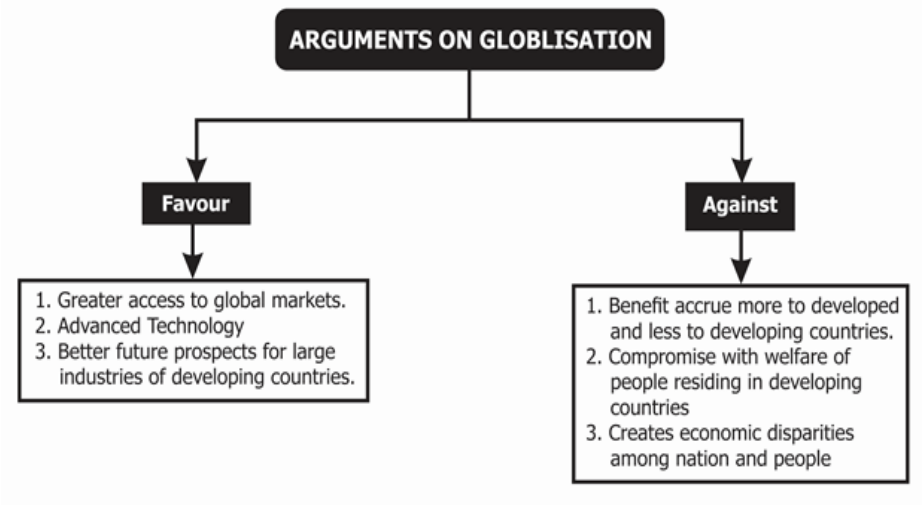
Globilization is important for the financial and economical development of any developing country. One of the most important factor of globalization is that it increases the interactions between region and population around the globe. Globilization is also important as it increases the competition level among the companies and it lead to lower down the prices and provide various variety to the consumers also. Lower cost help in the financial and economical development growth of any country. The main characteristics of globalization is that it increase connectivity among the nations, improves standard of living, reduced production cost. As earlier it has been discussed the term globalization arise in fifteen centuary. Globilisation has been introduced in India in 1990 .Globilisation has been introduced in various sectors such as petroleum, steel, textile, pharmaceuticals, BPO. There various types of globalization such as Social Globilisation, Technological Globilization,,Economical Globilization and Financial Globilisation.. It also put tremendous impact on social, political, monetary areas. Globilisation also increase due to the improvement of transportation

***Assistant Professor, IFTM University Moradabad.**

and information technology. Globilsation is reguired to the financial growth of the developing country .It improves income savings and opens the doors of employment in developing countries. Globilisation provide work to the rural and poor people and the new advanced technology system provided better facilities to the consumers as it increase the competition among the industries and provided various varieties to the consumers. Globilisation provide access to the new markets and new talents and the way of standard living has also been raised.It also opens the doors to the foreign trades to do the investment in the developing countries .Globilisation gives opportunities to new markets to expand their business into foreign trade purpose. It also enhances the global cooperation and tolerance.It also increases the economical growth of the country. Globilisation also improve the financial economy of any nations which leads to the development.

Impact of Globilization

- **Outsourcing:** This is one of the most common factor of globalization a company often recruits regular service from outer sources.(like legal advice ,computer service etc. Many services like BPO, BPS and call centres which have voice based services being outsourced by the companies to the advanced country to India.



- **High Standard of Living:** With the outbreak of globalization the financial and economical growth of India has increased and thus the standard living of an individual has also increased. Hence therefore many cities are undergoing a better standard for living with business development.
- **Increase Competition:** Due to globalization the level of competition increase as compare to the domestic companies this provide a various to the consumers at a very low price .

Advantages of Globilisation

1. Better Finances.
2. Great Development
3. Increase Standard of living
4. Decrease Poverty
5. Better job opportunities
6. Better Technologies.
7. Increase the flow of information between the developing countries.
8. Increase the competition and provide various varities to the consumers.
9. Impact on Agricultural Sector.

Disadvantages of Globilisation

1. Increase crime rate
2. Loss of jobs in underdeveloped countries.
3. Technologies take place of human resources
4. Communicable disease are spreading over world .
5. Unemployment give rise to different crime such as Money Laundering, Human Trafficking,
6. Increases the rate of cyber crime.

How Globilisation Increase the Crime Rate

Globilisation is important for social, economical and financial growth of any developing countries but the bitter side of this part as it lead to various crime like Money laundering, Human trafficking, Cyber crime, Counterfeiting of various goods to the European Countries, Providing drugs to various countries ,Corruption, Violating war like Terrorism. This crime usually expand after the interference of unnecessary advanced

information technology and due to the illegal immigration of labours to the foreign countries give rise to human trafficking .Every Nation has to pay the consiquences for the financial growth .Economical Globilisation expand the bridge between the rich and the poor. Industrilization and Privitization are some how responsible to prevent these crimes.

1. **Money Laundering:** Money laundering is the process of illegally concealing the origin of money obtained from illicit activities such as gambling, corruption drug trafficking and converting into legitimate process. Criminals use various techniques to disguise their origin of money. This will lead to the origin of white collar crimes. Bigger industries save their taxes and expand all the money into foreign trades and this will lead to the tax invasion crime.
2. **Cyber Crime:** Globilization also increases the rate of cyber crime. No doubt that ICT and globilization help in the developing groeth of the country but it also leads to the cybercrime.Innovations and advancement .ICT provides developing extraordinary chances for providing developing educational programmes,better policy formation and implementation.The entire world is getting digital and whole world is transforming and globilising day by day. Hence it lead to increase in cyber crime.As a ssresult the cyber crime put attack on information of individual,organizations and government as well.It may lead to "Cyber Theft ,Cyber Bullying and Cyber Defammation and Cyber Terrorism,Extortion Cyber Forgery and Fraud and Pornography Content also.Now these days the criminals use to leake all the personal information related to privacy and important documents of not only of an individual but also related to organisation and government policies and this create cyber threat mong the nations and this is the biggest problem the nation is facing near by.The biggest achievement of globilisation in related to cyber is **Artificial Intelligence**.It is a field of research of computers in related to advanced technology that studies and research various methods of software systems .Some high profile example of artificial intelligence in related to search engines is "**Google** recommended system such as **Netflix** ,**Youtube** followed by human interacting speech such as **Alexa**. This is the most advanced technology in artificial intelligence. Artificial Intelligence has been commonly used in various field. There are some disadvantage of artificial intelligence suh as highly costs, Unemployment ,Encourging Human Lazziness.
3. **Terrorism:** Globilisation also increase the rate of terrorism

among world wide.This is not hidden that globilization provide a better outcome sources for various countries for the financial and economical development many people find globilization cause benefit to them but some people around the people being threatned by the process of globilization as it causes global terrorism around the world.Globilization increases the incentives and opportunities for terrorism and facilitate the organization.

4. **Human Trafficking:** Human trafficking is the biggest example of how globilization increase the facilitate growth of the developing countries and increase in international crime for the economical gain.Human trafficking affect the global economy as labour supplies and transmit for the illegal immigration.Womens and Childrens are the most exposed part of the human trafficking caused by the globilization.These turn into commodities and selling human being into international market.It occurs both transtionally and domestically over world wide.
5. **Corruption:** Globilisation also increases the rate of corruption. Corruption is recognized as a critical issues between the globilizing and the economical development .The main cause of the globilization penalize the economical development asit limit the citizens to access esssential goods and services as globilization increase the competition level and provide various varieties to the consumers,thus it cause increase in the corruption.Corruption potentiate specially in under developed countries .India is in the 93 rd position according to the Corruption Prevention Index in year 2023 and dropping down to 85 th position in year 2022.Denmark ,New Zealand,Finland perceived as the leased corrupting nations among the world.
6. **Counterfeiting:** Counterfeiting leads to the substantial economical loss to government as well as buisness also.It deprives thre legimate buisness to the economical growth .Legtimate buisness give rise to losses jobs and it increase the crime rate and unemployment also.Conterfeit products also put affects on pharmaceuticals industries and pose severe risk to consumer health and safety.Fake products lead to quality control and cause health hazard.

Role of Counterfeiting in National Security

- **Funding Criminals and Increase Terrorist Activities:** Counterfeiting plays an important role for the funding if criminals and terrorist activities. This can cause severe damage to the

national security.

- **Intellectual Property Rights:** This will lead to unauthorized reproduction of intellectual property rights such as trademark, copyright,geographical indications.The theft of intellectual property undermines the innovation and competitiveness of national industry.
- **Cybersecurity Threats:** Counterfeiting of goods increasing through online platform this contributing the growth of cyber crime.The sales of fake products through online may lead to the personal information of an individual causes potiential risk to the individual and business also.
- **Drug Trafficking:** Globilization lead to the drug trafficking which involve illegal trade and transporation of narcotics substances across the international borders and with in countries.Economical disparities and Unemployment are the various of drug trafficking.There are various countries with increase rate of drug trafficking like Afganistan,India ,The Bahamas,Columbia,Costa Rica,Pakistan,Panama.Drug abuse is a global phenomena affecting various countries but its extent and characteristics differ from region to region .India is also caught in the circle of these drug abuse and the number of drug addicts increasing day by day.
- **Globilisation Causes Crime Against Women:** Globilization not only causes the financial and economical growth of the developing countries but the advancement of new technology and advancement lead to liberalization and privatization and employment of women lead to the new growth of crime against the women.The analysis of violence and crime during these days against the women in these days along with the social,economical,developmental and political discrimination against the woman.India is the present case of the social, economical, developmental and educational growth of the women along with thev policy and legislative growth measures. To tackle this problem various act such as Domestic Violence, Sexual Harrasment of Women at work place has been passed by the Indian Government to take necessary step against these crimes. There are 33,764 rape cases in India in year 2013. The rate of crime increased in year 2014 and decreased in year 2015. A number of crime against women related to rape, sexual harassment of women at work place Abduction, Dowry Prohibition Act. The crime rate increased after globalization in India.

Globilization and Transnational Crime: Globilization has lead to increase volume of legitimate cross borders financial transtitional and allows the criminals to process the crime so easily. Globilisations also facilitates new opportunities between terrorist and transnational organized crime. The ability of terrorist to move towards the financial resources and weapons to commit terrorist activity. The following steps are to be taken for transnational crime related to globalization.

1. **Open Market:** Every Nation open their market for foreign countries for trade and business so that foreign traders enter into country for investment and it is not easy to trace each other and unfortunately it increased the crime.
2. **Liberalisation:** Due to the liberal policies of globilisation the crime rate has been increased.
3. **Privatization:** It means giving control to the private sectors. There are some negative effect of privatization as it increase bribery and corruption and decrease transparency in business. It also expand the bridge between the rich and the poor.
4. **Globlisation in Criminal Law:** The effect of globilisation in social phenomena lead to changes in the society. Today many socio-economic changes has been noticed due to the effect of globilisation like peace, crime, immigration, unemployment, terrorist activities technological development and environmental threats, pandemics (Covid 19),income distribution and prosperity. International law, Interntional trade law are affected by the globilisation. Globilisation has influenced everything crime, criminal, victim and how to commit the crime. Globilisation has created new challenges. The invention of computers which is sometime useful but it create some negative impact to the individual, organization and government also. This will lead to cyber crime and criminals sometime difficult to detect through cyberspace. The internationalization of the world and the borders has created new opportunities for the criminals.The evolution of the computer networks help to transfer huge funds at a moment. One of the most important thing that the government acted to take simultaneously action against these crime. Other crime such as Drug Smugling, Sexual Terrorism, Human Trafficking takes place. The second obstacle will be the Cultural Relativism considers the determination of the principle related to custom, tradition, religion.These relativism give rise to violating the principles of human rights.Criminology and Decriminalization in

a globalized value system are based on the principles of human right system. Today the large number of criminal titles increase the fear of criminal threats. Global cyber crime, Cyber Terrorism has been increasing day by day and put their impact on every individual, organization, business and government.

The globalization of crime is one of the major factor of criminal inflation and put their negative effect on industries, technology advancement and different systems of law. But the most important part of this that the fear of the crime leads to exteme criminalization and put their negative effect on the individual's security and personal information.

Objective of the Study

The main objective of the research paper are as follows:

1. Does globilisation increases the crime rate.
2. Rate of Terrorism increase in India after globalization.
3. What are the Indian Laws that dealing with the transnational crime.
4. Is globilisation responsible for unemployment and corruption.
5. Is India take any necessary step to control the crime that occur due to globilisation.
6. What steps should be taken by India to control the crime that occur due to globilisation.
7. Is globilisation responsible for increase in cyber crime especially in case of Artificial Intlligence.

Conclusion

Globilisation arise in fifteen centuary and in India it is introduced in year 1990. Globilisation is necessary for the social,economical development of the country.Globilisation and Urbanization brought new challenges all over the world.It changes the trade business, information technology advancement, people communication world wide,expanding trade opening markets to the foeign traders fo the business purpose and providing access to the natural resources and markets and labour markets.As earlier it has been mentioned that it provide global competition world wide that lower down the prices and provide various varieties to the consumer at a very low price.Globilisation is important as it provide employment in public sectors.It also improves the international relations that occur due to the foeign trade and business

across world wide. The main disadvantage of globilisation is loss of jobs in under developed countries that increase the crime rate and in case of transational crime it expand the bridge between the rich and poor. People dependant on each other for their work to be done. Manual labour has been decreased due to the advancement of information technology. Big Companies getting more powerful as compare to small companies and big companies not paying enough tax to world wide and this will lead to white collar crime like Money Laundering, Globilization causes immigration of labours and this will lead to Human Trafficking. Due to the advancement of the information technology cyber crime has take place.

The government has to take necessary action against to prevent the crime that occur due to globilisation is to make some laws related to prevent some crime that occur due to globalization and make some necessary measures to control these crime such as Drug Trafficking, Terrorism, Corruption, Sexual Harrasment of Women at Work Place.

Globilisaton is important for social,economical and financial development and it is necessary for the developing countries like India so it is not required to stop globilisation as it important for the economy of the development of any nation and provided various jobs opportunities to the individual's .So one should take the proper control measures the negative impact of globilisation as it does not create any threat to the nations as well to the individuals, organization and business.

To stop the terrorist activities that occur due to globilisation illegal funding of foreign trades to be stopped . In India "Terrorist Act and Unlawful Activities (Prevention Act)1967 has been passed to contro the terrorist activities in India.

To control bribe and corruption that occur due to unemployment in underdeveloped countries through globalization manual work should be come into force as individual depend upon advanced technology system this lead to rise in loss of jobs and it will result into crime. Globilisation increase the rate of cyber crime that will lead to pornography, cyber stalking. Globilisation give rise to the advanced technology of Artificial Intelligence. This technology is necessary for the development of social and economical development of the country but are there are few disadvantages of artificial intelligence such as it increase the rate of unemployment.

To control the sexual abuse of women certain laws has been passed by the Indian government such as "Domestic Violence Act 2005 and Sexual Harrasment of Women at Work Place.

To avoid human trafficking there should be some necessary steps to be taken as the illegal immigration of labours in foreign traders should be controlled and safety measures taken by the "Human Rights Commission .

So, finally the conclusion of the research paper is that globilisation is necessary for the financial economy of the country but the crime that occur due to the negative impact of globilisation must be stopped.If the world come together to control these negative measures and to find a solution these crimes can be prevented.

Bibilography

- https://ivypanda.com/essays/current-trends-of-globalization-of-crime/
- https://www.researchgate.net/publication/228381107_Globalisation_and_crime
- **http://** www.questjournals.org
- https://www.e-ir.info/2020/09/16/globalization-and-transnational-crime/#:~:text=And%20while%20globalization%20has%20led,now%20available%20via%20the%20Internet.
- https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf
- https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5960&context=libphilprac
- https://www.researchgate.net/publication/329862526_TRANSNATIONAL_ORGANIZED_CRIME_IN_INDIA_A_NEW_FRAMEWORK_OF_ANALYSIS

◆ ◆ ◆

14.

Difficulties of Protecting Individual Rights in Artificial Intelligence

M. Mahisha Malar & Selgin. B***

Introduction

Artificial Intelligence (AI) is one of the 21st century's most revolutionary technical developments, changing everything from communication and business to healthcare and government. AI systems' ability to evaluate enormous volumes of data and make decisions on their own present unmatched prospects for efficiency and creativity as they become more and more integrated into daily life. But there are also a lot of difficulties associated with this quick spread, especially when it comes to defending individual rights. The relationship between artificial intelligence (AI) and human rights is complex, with the promise of technological advancement frequently at odds with the core values of justice, privacy, and autonomy. Artificial intelligence (AI)-powered surveillance tools, including face recognition software, have the ability to track and observe people without their permission, creating a widespread feeling that people are being observed. When used by businesses or governments, these technologies have the potential to violate people's right to privacy, which is a basic human right protected by international law. These privacy concerns are further exacerbated by the expanding use of AI in the collection

***Assistant Prof., of Law, CSI ILS, Parassala.**

****CSI ILS, Parassala**

and analysis of personal data for commercial purposes, such as targeted advertising. Businesses frequently compile enormous volumes of data to profile people and forecast their behaviour, which can come out as intrusive or manipulative.

This undermines efforts to secure personal information. This begs the question of how to strike a compromise between the requirement for data to power AI systems and the necessity of maintaining individual privacy rights. The Risks of AI Bias and the Danger to Autonomy Beyond privacy, AI seriously jeopardizes personal freedom. One of the main components of personal freedom is autonomy, or the capacity for people to make choices without external pressure. But this autonomy may be threatened by AI's expanding influence in decision-making processes, which span from credit rating to hiring. Social media companies, for instance, use AI algorithms to curate material that gradually modifies users' experiences by influencing their beliefs and behaviours. This affects not just the Caliber of information people get but also has the potential to influence their judgments in ways they may not have selected on their own.

Furthermore, a major danger to autonomy and justice is the inherent prejudice in AI systems. Since AI algorithms are usually taught on historical data, they may exhibit biases reflective of the current society. AI may reinforce and even magnify these prejudices if they are not appropriately addressed, producing discriminating results. For example, skewed training data reflecting historical discriminatory practices has led to criticism that AI systems employed in employment procedures Favor some demographic groups over others. This poses important concerns about how to make sure AI systems don't perpetuate current injustices or invent new kinds of prejudice. The intricacy of numerous AI systems, sometimes known as "black boxes," adds to the difficulty of safeguarding individual liberties. Decisions made by AI systems that have an impact on people's lives are frequently not evident from the outset, making it challenging for humans to contest or appeal them. People's sense of control over their lives may be diminished by this lack of transparency, which can also erode trust in AI systems.

Finally, defending individual rights in the AI era is a difficult task with many facets. It is crucial to address the ethical and legal ramifications of AI use as it develops and becomes more integrated into all facets of society. Ensuring fairness, maintaining autonomy, and protecting privacy are essential elements of this endeavour. To overcome these obstacles and guarantee that AI is created and applied in ways

that respect and defend individual rights, technologists, legislators, and civil society must work together in a coordinated and cooperative manner. We can only fully utilize AI while preserving the principles that guide our society if we take this approach.

Individual Rights in India[1]

Articles 12-35 of the Indian Constitution explain the rights of Individual which is also known to be Fundamental Rights of the country which the state must preserve.

Individual Rights Include

Right to Equality (Article 14-18)

Right to Freedom (Article 19-22)

Right against Exploitation (Article 23-24)

Right to Freedom of Religion (Article 25-28)

Cultural and Educational Rights (Article 29-30)

Right to Constitutional Remedies (Article 32)

Fundamental rights are considered to be important because they are the backbone of the nation. It is necessary to protect the interests of the people.

Ways in Which AI Affecting Individual Rights

Privacy Challenges in the Age of AI

Many sectors have undergone radical change as a result of artificial intelligence (AI), which offers previously unheard-of efficiency and creativity. But there are serious privacy concerns associated with this technical breakthrough, especially when it comes to the enormous volumes of data needed to run AI systems. Concern over the possible erosion of privacy is growing as AI technology become more commonplace. Data is the lifeblood of AI systems, particularly sensitive and personal data. These systems require access to large datasets in order to work properly; these datasets frequently contain information about people's preferences, activities, and even biometric information like speech patterns or face traits. Because of our reliance on data, personal information is being collected and stored in large quantities,

1. Dr. J.N. Pandey, Constitutional Law of India 59 (Central Law Agency, Allahabad, 52th edn., 2015).

which begs important concerns about how it is maintained, who can access it, and why.

AI's potential for widespread spying is one of the biggest threats to privacy. AI-powered devices, such sophisticated monitoring tools and facial recognition software, allow for hitherto unheard-of levels of surveillance. These technologies give governments and businesses the ability to follow people around, keep an eye on what they do, and even forecast their behaviour. This degree of surveillance may cause one to lose their sense of anonymity and experience a constant sense of being watched, which may be frightening to one's ability to express oneself freely.

Moreover, even anonymized data may be exposed due to AI's ability to swiftly evaluate and process enormous volumes of data. In order to re-identify someone, advanced AI systems may cross-reference anonymised datasets with additional data, jeopardizing their privacy. The risks associated with data breaches and unauthorized access are increased by this re-identification risk, which also calls into question the efficacy of more established privacy protection techniques like data anonymization.

The extensive commercial application of AI raises privacy issues as well. Businesses frequently gather and examine personal information in order to target ads, customize services, and forecast customer behaviour. Although this may result in more customized user experiences, it also brings up moral concerns of manipulation and consent. People might not be aware of how or to what extent their data is being shared with third parties or used.

Because of these difficulties, there is an increasing need for strong ethical standards and privacy laws that specifically address the concerns associated with artificial intelligence. Robust data protection regulations and increased openness on AI system functioning are necessary for safeguarding privacy in the AI era. People should have the power to control their personal information and be informed about how it is gathered, used, and preserved.

In the end, protecting privacy will be a crucial issue that needs constant attention from legislators, developers, and society at large as AI continues to advance. To ensure that AI research advances in a way that respects and preserves fundamental human rights, it is imperative to strike a balance between the advantages of AI and the need to protect individual privacy.

Bias and Discrimination in AI Systems

Artificial Intelligence (AI) has enormous potential to promote efficiency, fairness, and creativity in a variety of fields. But even with all of its promise, AI is not impervious to the prejudices that are present in human culture. As a matter of fact, AI systems have the potential to reinforce preexisting prejudices and create discrimination in vital domains like lending, recruiting, and law enforcement. This happens because human input and historical data are frequently used by AI systems in their development, which can accentuate and incorporate biases either in the data or in the algorithms themselves.

The root of bias in AI are the large-scale datasets are used to train AI systems, especially those built on machine learning, to find patterns and make judgments. Nonetheless, the biases included in these statistics are a reflection of historical and societal realities. For instance, if hiring data is used to build a machine learning model that demonstrates a preference for male candidates, the AI system may be programmed to perpetuate gender prejudice by favouring male candidates in subsequent hiring choices. Similarly, an AI system in law enforcement may continue to target minority communities disproportionately if the data used to train it reflects racial profiling.

In AI, bias may also originate from the algorithms. Biases may be introduced into an AI system by its design, which includes the attributes the system prioritizes. For example, an AI system used for loan approvals may unintentionally discriminate against people who are less likely to have certain attributes because of systemic inequality if it is built to consider factors that are more accessible to certain demographic groups, like home ownership or higher education credentials.

Secondly, Discrimination in Hiring. AI systems are being utilized more and more in the employment process to conduct interviews, evaluate resumes, and even make the ultimate hiring decisions. Even while these programs are frequently marketed as being more impartial than hiring agents, discrimination may nevertheless be sustained by them. This happens when the algorithm is not built to take diversity into account, or when the AI is trained on skewed historical data. An AI resume screening system, for instance, can unintentionally disadvantage candidates from non-traditional or underrepresented backgrounds by learning to prefer applicants with particular work experience or educational backgrounds.

Furthermore, by linking particular characteristics to success in

specific occupations, AI systems have the potential to perpetuate prejudices. An AI system may give preference to applicants who match a certain demographic if it discovers that white men made up the majority of the company's previous successful workers. This would continue the lack of diversity in the workplace. In addition to having an impact on the individual, this form of prejudice can keep businesses from gaining from the unique viewpoints and skills of their workforce.

Thirdly, Discrimination in Law Enforcement. There has been much discussion on the application of AI in law enforcement, especially in light of its potential to worsen racial and ethnic discrimination. Among other things, AI technologies are utilized in facial recognition, predictive policing, and sentence suggestions. Unfortunately, these algorithms frequently produce biased results because they rely on data that reflects preexisting biases in the criminal justice system.

Predictive police algorithms, for instance, use past crime data to pinpoint locations where crimes are most likely to happen. But if the historical data is skewed, for example, by showing that minority neighbourhoods are overpoliced, the AI system would keep allocating law enforcement resources to such areas, which would create a vicious cycle of heightened monitoring and arrests. Systemic racism may be sustained as a result of the disproportionate targeting of minority populations.

Another domain in which prejudice resulting from AI bias might occur is facial recognition technology. According to studies, facial recognition software frequently misidentifies people with darker skin tones, which increases the number of false positives for people of color. Serious repercussions may result from this, such as false arrests and a decline in confidence in the criminal justice system.

Fourthly, AI is being utilized more and more in the financial industry to determine loan approvals, calculate interest rates, and evaluate creditworthiness. Although AI could improve the efficiency of loan decisions, if not handled appropriately, it could also reinforce discrimination. Artificial intelligence (AI) lending systems frequently rely on information that can be impacted by systemic disparities, such as credit scores, income levels, and historical borrowing patterns.

For example, past economic inequities, restricted access to financial services, or discriminatory lending practices may have resulted in poorer credit ratings for members of underrepresented communities. An AI system may arbitrarily reject loans to certain people or provide

them less favourable conditions if it ignores these criteria. Because fewer people who need it most can access capital, this can prolong economic inequality.

Furthermore, AI systems may unintentionally support redlining, a practice in which some neighbourhoods—many of which are mostly populated by minorities—are routinely denied access to advantageous loan terms. The AI may continue to discriminate against applicants from these areas and deepen economic inequality if it is trained on historical lending data that contains redlining.

Legal and regulatory systems also need to change to meet the particular difficulties brought up by AI. Institutions and governments must set rules to guarantee that AI systems are created and used in ways that uphold justice and safeguard individual rights. This could entail specifications for bias testing, openness in algorithmic judgments, and channels for people to object to biased AI results.

In summary, artificial intelligence (AI) has a lot of potential, but it also has the ability to reinforce preexisting biases and create new ones, which might result in discrimination in vital sectors like lending, hiring, and law enforcement. It is crucial to address these biases early on and make sure that AI systems are developed and deployed with fairness and equality at their core in order to maximize the benefits of AI while lowering its risks.

Transparency and Accountability in AI Decision-Making

The need for accountability and transparency in AI decision-making processes has increased dramatically as AI is incorporated into more and more facets of society. The capacity to comprehend and elucidate an AI system's decision-making process is known as transparency in AI. This is especially difficult because a lot of AI models especially those that are based on deep learning which involve complex mathematical networks that are difficult for people to understand. Large volumes of data are processed by these models in order to spot trends and reach conclusions, but the inner workings of these systems are frequently too intricate to completely comprehend. For example, while determining an applicant's creditworthiness, an AI system used for loan approvals may take into account hundreds of criteria. It might be challenging to identify or justify the precise set of circumstances that resulted in a decision, even when the outcome such as a loan approval or denial is obvious. Because they are unable to comprehend the reasoning behind the decision, those impacted by AI choices may find themselves in

situations where they are unable to contest or appeal the conclusion.

To make matters more complicated, a lot of AI systems are proprietary. Transparency may be further limited by companies' reluctance to reveal the inner workings of their AI models because of worries about intellectual property. This confidentiality may hinder external control and audits, which are essential to guaranteeing the impartial and moral operation of AI systems. Equally difficult is the accountability challenge in AI decision-making, especially when harm is done. AI systems are capable of making choices that have a big influence on people's life, like credit score determination, criminal justice sentencing, and job chances. If these choices result in negative consequences, such prejudice, erroneous arrests, or unjust rejections, it becomes difficult to assign blame.

The assignment of duty is made more difficult by the independent nature of AI systems. Which parties should have the responsibility: the AI system itself, the businesses that implemented it, or the developers who built the AI? As traditional legal systems were not intended to tackle the particular issues provided by AI, they frequently find it difficult to address these questions. There is a rising need for precise rules and laws that outline accountability in AI decision-making in order to solve these issues. This entails putting in place procedures that guarantee AI systems are auditable, transparent, and accountable as well as giving those impacted by AI choices a way to contest and seek compensation for unfavourable results. In the absence of such safeguards, the swift development of artificial intelligence may result in pervasive concerns about injustice, bias, and mistrust towards these potent tools.

Autonomy and Manipulation: The Impact of AI on Free Will

Artificial intelligence (AI) raises serious questions regarding human autonomy and free will since it has the potential to profoundly impact human behaviour and decision-making. With the rising sophistication and integration of AI systems into everyday life, such as recommendation engines, targeted advertising, and social media algorithms, people's decisions are being influenced by these systems, frequently in imperceptible and subtle ways. Sometimes, this influence goes too far and becomes manipulation when AI systems push people in the direction of particular choices, so compromising their autonomy.

The Influence of AI on Decision-Making AI systems are made to maximize results according to predetermined objectives, like boosting

sales, enhancing efficiency, or optimizing user engagement. In order to accomplish these objectives, artificial intelligence (AI) systems analyse enormous volumes of data on personal preferences, behaviours, and routines. They then use this data to forecast and impact future actions. To keep users engaged for longer, social media sites, for example, utilize AI to generate content feeds based on their interests. Similar to this, AI is used by e-commerce sites to recommend products based on a user's past browsing activity, encouraging them to make a purchase. These applications raise questions about manipulation even though they can improve the user experience by offering individualized content. Artificial intelligence (AI) systems may give preference to content or items that elicit strong emotional reactions, such fury or desire, above those that are in line with the user's true interests or values, if their goal is to maximize engagement or profitability. This can ultimately compromise people's autonomy by forcing them to make decisions that they otherwise might not have taken.

Manipulation and the Erosion of Free Will

The influence of AI is especially subtle, which is worrisome. In contrast to overt coercion, AI manipulation frequently occurs covertly, making it challenging for targets to identify and reject. Recommendation algorithms on streaming platforms, for instance, may gradually shape viewers' ideas by directing them toward content that supports particular points of view. In severe situations, this might result in "echo chambers" or "filter bubbles," where people are only exposed to data that confirms their preexisting opinions, which impairs their capacity to make free-thinking, well-informed judgments. AI-driven personalization can also produce a feedback loop in which an AI system's ability to predict and influence behaviour improves with the amount of data it gathers. As a result, options may become more limited as the AI continuously adjusts suggestions to fit user preferences, which may discourage experimentation and lessen the variety of experiences.

Safeguarding Independence in the AI Era

The implementation of safeguards that provide transparency, accountability, and user control is vital in order to preserve personal autonomy amidst the increasing impact of artificial intelligence. Users must to be able to choose not to be included in specific personalization or recommendation systems, as well as be informed about how AI systems are influencing their decisions. Furthermore, in order to guarantee that AI systems put user welfare and individual autonomy ahead of solely

profit- or engagement-driven objectives, ethical standards and laws are required. In conclusion, artificial intelligence (AI) presents serious hazards to individual autonomy and free will even while it has the potential to improve decision-making and user experiences. Addressing these dangers is essential to ensuring that people maintain control over their decisions and are not unintentionally influenced by forces beyond their control as AI grows more and more integrated into daily life.

Legal and Ethical Frameworks for Protecting Rights in AI

Strong ethical and legal frameworks are more important than ever to safeguard individual rights as artificial intelligence (AI) develops and permeates more facets of society. Even while artificial intelligence (AI) has many advantages, including better efficiency, healthcare, and personalized services, there are also major hazards to privacy, autonomy, justice, and responsibility. Sadly, there are still a lot of inadequate or out-of-date legal and ethical frameworks in place, which leaves holes in protection that require attention.

The Need for Robust Legal Frameworks

The swift advancement of AI technologies often outpaces the current legal frameworks. Many of these regulations weren't intended to handle the particular problems that AI presented because they were developed long before AI became widely used. For instance, in a world where AI systems are able to process and analyse enormous volumes of personal data to make judgments or predictions about specific people, standard privacy regulations could not be sufficient to safeguard people. People are exposed to misuse of personal information, data breaches, and privacy violations as a result of this gap.

Furthermore, it's common for current legal frameworks to lack precise guidelines about culpability for harm caused by AI systems. For example, it may not always be evident who is at fault when an AI-driven decision-making process produces discriminatory or inaccurate results—the AI itself, the developers, or the users. This ambiguity erodes confidence in AI technologies and makes seeking redress more difficult. To allocate blame and guarantee that people have options when AI systems abuse their rights, explicit legal norms are required.

The Need for Ethical Guidelines

Robust ethical criteria are important to guarantee that AI is created and implemented in a way that upholds human rights and fosters equity,

in addition to legal safeguards. Artificial Intelligence Development should be guided by ethical concepts including responsibility, openness, and non-discrimination. But in the absence of legally binding norms, moral principles are frequently disregarded or applied inconsistently.

The possibility for AI to be utilized in ways that deceive or hurt people, as well as bias in AI algorithms and the transparency of AI decision-making processes, are all concerns that ethical frameworks must address. These rules should also guarantee that a variety of stakeholders, particularly members of marginalized populations who stand to lose the most from prejudiced or discriminatory AI systems, are included in the development of AI technologies.

Addressing Insufficiencies in Current Frameworks

There is an increasing need for international cooperation and conversation to overcome the shortcomings in the legal and ethical frameworks that exist today. AI is a worldwide technology, and country boundaries are frequently crossed in its development and application. Therefore, uniform international standards are required to guarantee the protection of individual rights across state borders. To ensure that human rights and ethical considerations are given priority in AI development, governments, tech corporations, and civil society organizations must collaborate to establish and implement these standards.

In conclusion, even though artificial intelligence (AI) has a lot of promise, effective protection of individual rights will require strengthening the ethical and legal frameworks that control its use. These frameworks must be maintained and modified as AI develops in order to satisfy the demands of this brand-new technological environment and guarantee that AI advances society without violating basic human rights.

conclusion

Navigating the Complexities of Protecting Individual Rights in AI

As Artificial Intelligence (AI) rapidly advances and becomes deeply embedded in our daily lives, the protection of individual rights has emerged as a critical concern. While AI offers enormous potential for innovation and societal benefit, it also poses significant risks to privacy, fairness, autonomy, and accountability. The challenges discussed—ranging from privacy invasions to biased decision-making and the erosion of personal autonomy—highlight the urgent need for comprehensive

strategies to safeguard individual rights. The complexity of these challenges lies in the dual nature of AI that it can both enhance and undermine human rights, depending on how it is designed, deployed, and regulated. The current legal and ethical frameworks often fall short in addressing the unique issues posed by AI, leaving gaps that can lead to the infringement of individual rights. As AI continues to evolve, these frameworks must be adapted and strengthened to provide robust protections. This includes updating outdated laws, developing clear guidelines on accountability, and ensuring that ethical considerations are at the forefront of AI development.

Moreover, transparency and accountability in AI decision-making processes are crucial to maintaining public trust and ensuring that individuals have control over their data and decisions. Addressing these challenges requires a collaborative effort among governments, technology companies, and civil society to establish international standards and best practices.

In conclusion, while the difficulties of protecting individual rights in the age of AI are formidable, they are not insurmountable. By proactively addressing these challenges and creating robust legal and ethical frameworks, we can ensure that AI serves humanity in a way that upholds and respects individual rights. The goal should be to harness the power of AI while minimizing its risks, ensuring that this transformative technology benefits everyone without compromising fundamental human freedoms.

◆ ◆ ◆

15.

The Intersection of Artificial Intelligence and Legal Practice: Exploring the Future of Legal Services in Banking and Financial Sectors

Ms. Neha Prajapati & Ms. Vinit Raikwar***

Introduction

Artificial Intelligence (AI) is increasingly becoming a transformative force in the legal profession, reshaping traditional practices and introducing new methodologies for managing legal tasks. This section explores the integration of AI in legal practice, its various applications, the benefits it offers, the challenges it presents, and its potential impact on the future of the legal profession. Artificial Intelligence (AI) has emerged as a transformative force in contemporary technology, fundamentally altering various industries and shaping the future of technological innovation. Its capabilities range from automating routine tasks to solving complex problems, and its impact is evident across a multitude of sectors. This overview provides a comprehensive look at AI's definition, key technologies, and its diverse applications in modern technology.

***Assistant Professor, Chameli Devi Institute of Law.**

****Assistant Professor, Chameli Devi Institute of Law.**

Overview of AI in Legal Practice

AI refers to the use of computer systems that can perform tasks typically requiring human intelligence, such as understanding language, recognizing patterns, solving problems, and making decisions. In the legal field, AI is being applied to automate and enhance various tasks that are central to legal practice, including research, document review, contract analysis, litigation support, and client interaction.

Evolution of AI in Law

- **Early Adoption:** Initially, AI in the legal sector was primarily focused on legal research, with tools like LexisNexis introducing basic search functionalities. Over time, advancements in machine learning, natural language processing (NLP), and predictive analytics have expanded AI's capabilities.
- **Current Landscape:** Today, AI tools are used not only for research but also for automating repetitive tasks, predicting case outcomes, managing contracts, and even advising clients. Law firms and legal departments are increasingly investing in AI technologies to improve efficiency, reduce costs, and enhance service delivery.

Artificial intelligence is increasingly transforming the legal industry by streamlining labor-intensive tasks. AI tools are now assisting lawyers in various domains, including due diligence, legal research, contract review, and litigation prediction. These applications not only enhance efficiency but also reduce the risk of human error.

AI Applications in Law Include

1. **Due Diligence**: AI tools like Kira Systems, LEVERTON, and eBrevia automate contract review, extracting key information to support faster, more accurate analysis.
2. **Legal Research**: Tools like ROSS Intelligence and Casetext's CARA assist in legal research, providing insights and recommendations by analyzing vast legal databases.
3. **Document Automation**: AI software automates the creation of legal documents based on predefined templates, saving time and reducing manual errors.
4. **Litigation Prediction**: AI can predict litigation outcomes by analyzing past case data, helping lawyers make informed decisions.

- **Intellectual Property Management**: AI aids in managing and analyzing large IP portfolios, offering insights to help lawyers navigate complex cases.
- **Electronic Billing**: AI automates billing processes, ensuring accuracy in tracking billable hours.

While these advancements offer significant benefits, they also raise concerns about bias in AI systems, emphasizing the need for ongoing scrutiny and multiple data sources to ensure fairness and accuracy.

This overview highlights the growing role of AI in the legal field, offering promising tools to enhance legal practice while also posing challenges that require careful consideration.

Prediction Technology

Prediction technology is increasingly used in legal practice to forecast case outcomes. Studies have shown that AI can often predict court decisions more accurately than legal experts. For example, a 2002 study by Washington University professors achieved 75% accuracy in predicting Supreme Court cases, outperforming experts at 59%. Later, in 2017, researchers including Prof. Daniel Katz achieved 70.2% accuracy on Supreme Court cases, while a separate study on the European Court of Human Rights reached 79%.

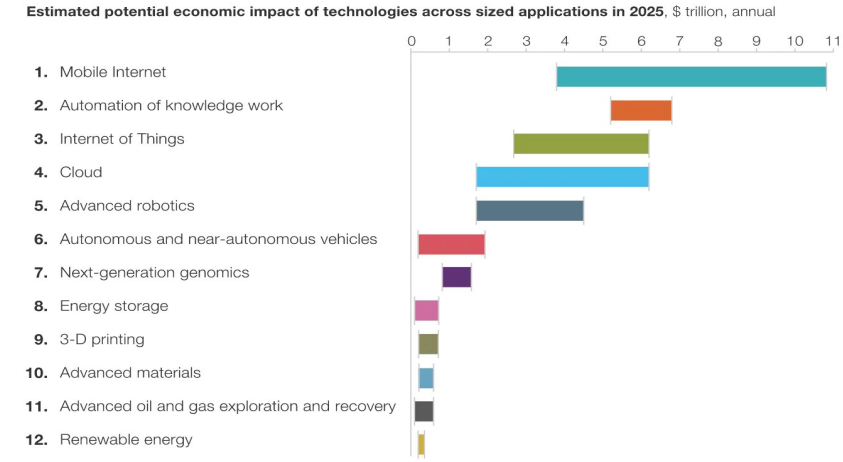
Several AI Companies are Leveraging Predictive Analytics in Law

- **Intraspexion**: Uses AI to detect early signs of litigation risk by analyzing documents and highlighting high-risk terms.
- **Ravel Law**: Analyzes case law and judge rulings to predict case outcomes and provide insights into a judge's decision-making patterns.
- **Lex Machina**: Offers analytics on case timing, lawyer experience, and outcomes before specific judges.
- **Premonition**: Claims to predict a lawyer's success by analyzing win rates, case durations, and judge pairings, although it highlights the complexity and data requirements for such predictions.

These tools require extensive data to function effectively, but they hold significant potential for enhancing legal strategy and decision-making.

Document Automation

A report by McKinsey & Company predicts that automation of knowledge work will be among the leading disruptors in the global economy.



SOURCE: McKinsey Global Institute

Exploring the Future of Legal Services in the Banking and Financial Sectors

Law graduates often face difficulties in securing employment, particularly when compared to their peers in STEM and management fields. While traditional career paths in legal practice, judiciary, academia, and research are well-trodden, the banking and finance sector is a less explored yet promising area, offering a diverse array of rewarding roles.

The banking and finance industry presents numerous opportunities for law graduates, ranging from legal officers and assistants responsible for managing legal data, to advocates specializing in bank litigation. Legal managers, especially in private sector banks, are pivotal across various areas. In corporate banking, they handle legal documentation, compliance, and regulatory matters, while in branch banking, they manage the legal aspects of everyday operations. However, the most lucrative opportunities are often found in litigation roles, which are widely available in cities of all sizes.

The Role of Legal Managers in Banking and Finance

Legal managers play a critical role in debt recovery, a fundamental function within banking. When customers default on loans, the onus

often falls on legal managers, who guide the judicial process and oversee panel advocates in the pursuit of outstanding debts. They employ a variety of legal tools, categorized into "soft tools" and "hard tools," to recover debts.

Soft Tools for Debt Recovery

Legal managers utilize several soft tools, including demand notices for overdue payments and loan recall notices for non-performing assets (NPAs). They also employ mediation and conciliation notices to encourage non-adversarial settlements and issue pre-litigation notices to escalate cases when necessary. These approaches enable banks to recover debts more efficiently without immediately resorting to litigation.

Hard Tools for Debt Recovery

When soft tools prove insufficient, legal managers turn to hard tools, initiating formal legal proceedings to recover debts. These tools include:

- **Alternative Dispute Resolution (ADR):** Methods such as arbitration and Lok Adalat provide resolution outside traditional courts. Arbitral awards can be enforced through civil courts, while Lok Adalats facilitate informal settlements.
- **Quasi-Criminal Proceedings:** Under the Negotiable Instruments (NI) Act, legal managers can initiate criminal proceedings for cheque payment defaults. Similarly, the Payments and Settlements Systems (PSS) Act allows for action against dishonoured electronic fund transfers.
- **Civil Proceedings:** Legal managers use laws like the SARFAESI Act and the Recovery of Debts and Bankruptcy Act to enforce security interests and recover debts through Debt Recovery Tribunals (DRTs).
- **Executive Magistrate Proceedings:** State-specific laws, such as the Madhya Pradesh Lok Dhan (Shodhya Rashiyon Ki Vasuli) Adhiniyam, 1987, enable expedited recovery processes before Executive Magistrates.
- **Insolvency Resolution under IBC:** In cases of significant defaults, legal managers can initiate insolvency proceedings under the Insolvency & Bankruptcy Code, 2016, safeguarding the bank's interests throughout the process.

Expanding the Career Path: How Law Graduates Can Secure Roles in Banking and Finance

To unlock career opportunities in the banking sector, law graduates should focus on the following steps:

- **Develop Expertise in Banking Laws:** Build a robust foundation in banking regulations, economic laws, and debt recovery processes.
- **Gain Practical Experience:** Intern with advocates empaneled with banks to gain first-hand experience in banking operations and legal challenges.
- **Engage in Pre-Placement Activities:** Participate in pre-placement talks and training programs offered by universities in collaboration with banks to network and align with industry expectations.
- **Enhance Technical Skills:** Develop proficiency in Microsoft Excel for data management and analysis—an essential skill for banking roles.

By focusing on these areas, law graduates can tap into a wealth of career opportunities within the dynamic and growing banking and financial sectors, where legal expertise is increasingly valued.

The Integration of AI in Legal Services for Banking and Finance

The banking and financial sectors are undergoing significant transformations driven by technological advancements, with Artificial Intelligence (AI) playing a pivotal role in reshaping legal services. AI's integration into legal practice promises to enhance efficiency, accuracy, and strategic decision-making while presenting new challenges and opportunities for legal professionals. Below is an exploration of how AI is influencing these fields and what lies ahead.

Current State of Legal Services in Banking and Finance

Legal services in the banking and financial sectors are essential for managing compliance, mitigating risk, and navigating complex regulatory environments. These services traditionally involve:

1. **Regulatory Compliance:** Ensuring adherence to financial regulations and standards, such as anti-money laundering (AML) laws, the Dodd-Frank Act, and international regulations.
2. **Contract Management:** Drafting, reviewing, and negotiating

contracts related to financial transactions, mergers and acquisitions, and investment agreements.

3. **Risk Management:** Identifying and addressing potential legal risks associated with financial activities, including litigation and regulatory investigations.
4. **Dispute Resolution:** Handling disputes arising from financial transactions, investments, or regulatory actions, often through arbitration or litigation.

Impact of AI on Legal Services in Banking and Finance

Enhanced Regulatory Compliance

- **AI-Powered Compliance Monitoring:** AI systems can continuously monitor transactions and financial activities for compliance with regulatory requirements. These systems detect anomalies, flag suspicious activities, and generate real-time compliance reports, reducing the risk of regulatory violations.
- **Automated Reporting:** AI tools can automate the generation of regulatory reports, ensuring accuracy and timeliness while minimizing manual errors.

Improved Contract Management

- **Contract Analysis and Review:** AI-powered tools can analyze and review contracts to identify key terms, potential risks, and compliance issues. These tools can also suggest modifications and ensure that contracts adhere to relevant regulations.
- **Contract Lifecycle Management:** AI can manage the entire lifecycle of a contract, from drafting and negotiation to execution and renewal, improving efficiency and consistency in contract management.

Advanced Risk Management

- **Predictive Analytics:** AI can analyze historical data and market trends to predict potential legal risks and financial impacts, allowing legal professionals to address issues proactively before they escalate.
- **Fraud Detection:** AI systems can identify patterns of fraudulent behavior and flag suspicious activities, helping financial institutions mitigate fraud risk and enhance security.

Efficient Dispute Resolution

- **Automated Dispute Resolution Systems:** AI can facilitate the resolution of disputes through automated negotiation and mediation platforms, streamlining the process and reducing the need for traditional litigation.
- **Legal Research and Case Analysis:** AI tools assist in legal research and case analysis by quickly identifying relevant precedents, statutes, and legal arguments, supporting more effective dispute resolution strategies.

Streamlined Client Interaction

- **AI-Powered Chatbots:** Chatbots and virtual assistants can handle routine client inquiries, provide basic legal information, and assist with document management, improving client service and efficiency.
- **Personalized Legal Advice:** AI systems can analyze client data and provide tailored legal advice based on individual needs and financial circumstances.

Future Trends in AI and Legal Services for Banking and Finance

Increased Integration of AI and Blockchain

- **Smart Contracts:** Combining AI with blockchain technology can enable the creation of self-executing smart contracts that automatically enforce contract terms based on predefined conditions.
- **Secure Transactions:** AI and blockchain can work together to enhance the security and transparency of financial transactions, reducing fraud risk and improving regulatory compliance.

Development of AI-Driven Legal Platforms

- **Integrated Legal Platforms:** Future developments may include comprehensive legal platforms that integrate AI with other technologies, such as data analytics and machine learning, offering end-to-end solutions for legal services in banking and finance.
- **Enhanced Predictive Capabilities:** Advances in AI may lead to more accurate predictions of legal outcomes and financial risks, supporting better decision-making and strategic planning.

Regulation and Ethical Considerations

- **AI Governance:** As AI becomes more integral to legal services, regulatory frameworks will be necessary to govern its use, ensuring ethical standards and protecting client interests.
- **Bias and Fairness:** Addressing potential biases in AI algorithms will be crucial to ensuring fair and equitable legal outcomes, particularly in areas like risk assessment and compliance monitoring.

Evolution of Legal Roles and Skills

- **New Legal Specializations:** The rise of AI may create new specializations within the legal profession, such as AI compliance officers and legal engineers, focusing on the intersection of technology and law.
- **Skills Development:** Legal professionals will need to develop expertise in technology and data analysis to leverage AI tools effectively and remain competitive in the evolving legal landscape.

The Future of AI and the Law

The initial integration of AI into legal practice marks the dawn of a profound technological disruption in the field. AI offers both immense opportunities and significant challenges to the legal profession, signaling one of the most transformative shifts since its establishment. As the impact of AI on legal practice continues to accelerate, it will increasingly take over billable hours, extend its application across a broader range of legal tasks, and necessitate a new skill set that many current attorneys may lack.

At present, adopting AI gives law firms and attorneys a competitive edge in terms of efficiency, cost-effectiveness, and productivity. However, this advantage will soon shift from being a leadership strategy to a necessity for survival. The widespread adoption of AI in law raises a host of critical questions. How will AI revolutionize law firm billing when tasks that once required weeks of billable hours can now be completed by AI in mere seconds? As AI takes over many routine tasks traditionally performed by junior associates, what will the repercussions be for hiring and career progression?

Legal education and training must adapt to prepare future lawyers for an AI-dominated legal landscape. The competitive balance between large, medium, and small law firms could be significantly altered. Might

businesses opt to bypass traditional law firms altogether and procure legal services directly from legal tech providers? Will AI systems face legal challenges for potentially engaging in the unauthorized practice of law? As AI systems increasingly rely on self-learning algorithms rather than predetermined instructions, the questions of how to ensure the accuracy, legality, and fairness of their decisions become paramount.

Will attorneys be held liable for negligence if they rely on AI that makes errors, or for malpractice if they fail to use AI that outperforms human capabilities? Could self-learning AI systems be required to testify in court to explain their decision-making processes? One thing is certain: those in the legal profession who embrace AI will prosper, while those who resist risk irrelevance. As one senior lawyer recently noted, "Unless private practice lawyers start to engage with new technology, they are not going to be relevant even to their clients." The AI revolution in law is here—now is the time to embrace it.

The Future of Banking: Regulatory Landscape

Financial markets are facing a more assertive regulatory environment, with a growing focus on consumer protection, data privacy, and the integration of AI into banking processes. As banks work towards implementing the Basel standards, the compliance window for these regulations will begin in 2025, with much of 2024 dedicated to preparation and implementation.

This evolving landscape is likely to lead to increased risk aversion among financial market participants, particularly as expanding customer bases and boosting profitability become more challenging. In response, banks must develop a detailed understanding of their customers' unique circumstances, ensuring that each is treated appropriately and in line with regulatory demands.

To strike the right balance between pursuing growth and fulfilling their prudential responsibilities, financial institutions will need to make significant investments in collecting customer-level data and enhancing engagement processes. Furthermore, recent updates from the Financial Conduct Authority (FCA), including the February 2024 guidance on the Consumer Duty Act, provide valuable insights into best practices and highlight areas needing improvement. These insights will be essential for businesses striving to meet new legislative requirements, enhance customer outcomes, and uphold higher standards of care.

Additional Responsibilities

Beyond debt recovery, legal managers defend the bank in consumer disputes, ensure compliance with regulatory requirements, and address issues related to fraud and counterfeit currency during loan repayment

Innovation In Finance and The Territoriality of Law

Innovation in Finance and the Territoriality of Law

The rise of money manager capitalism has transformed investment practices, adding a new layer of intermediation aimed at maximizing returns for fund holders. The global expansion of Eurodollar markets since the 1970s, alongside increasing financialization, led to a credit boom and substantial private wealth accumulation, fueling the growth of the asset management industry. Asset managers, now key players in financial markets, shifted from traditional investment strategies to more aggressive tactics focused on wealth shielding and tax engineering.

This shift spurred activity among finance companies but also marked the decline of shared prosperity. The debate in regional innovation studies over whether innovation is tied to specific regions or individual entrepreneurs has often assumed that large cities are the primary hubs of innovation. Indeed, major financial centers like New York, London, and Paris are seen as indicators of a region's ability to generate speculative capital flows.

However, the significance of International Financial Centers (IFCs) in fostering innovation extends beyond expertise and proximity. Legal scholar Katharina Pistor highlights how legal coding practices adapt to new asset classes, privileging certain asset holders through the enforcement of legal rights. Capital, contrary to traditional economic theory, comprises both an asset and a legal code, with the latter playing a crucial role in wealth generation. Lawyers use legal coding to shield assets from taxes and protect them from creditors, leveraging the state's legal framework.

Today's financial capital is predominantly encoded within leading IFCs like New York and London, underpinned by dominant legal systems such as English common law and New York State law. Trust and corporate law play pivotal roles in protecting and creating capital, with financial innovation in asset management heavily influenced by legal design. These legal-contractual constructs, including derivatives, bundle obligations and rights into increasingly liquid legal vehicles.

Specialized firms in finance, accounting, banking, and securities (FABS) shape the profiles of IFCs, focusing on private wealth creation rather than broader societal benefits. The role of these firms in global profit shifting and creative accounting underscores the darker side of financial innovation, exacerbating the crisis of the welfare state and raising concerns about the international corporate taxation system. Offshore havens like the Netherlands and Luxembourg, though recognized as tax havens in relation to other places, owe their status to the interplay between law and legal practice.

Pistor's research into the role of lawyers in creating private wealth reveals the profound impact of legal coding on the nature of financial assets. This transformation is driven by two key developments: the fragmentation of integrated business organizations and the expansion of legal territoriality, both of which are essential to understanding the evolving landscape of finance and innovation.

Review of Literature

Dörry and Hesse (2022). as discussed by This literature calls for a deeper engagement with the legal geographies of global finance, which are often perceived as innovative and are deeply rooted in legal frameworks. Additionally, it emphasizes the need for further detailed investigation into the complexities of financial vehicles and infrastructures across IFCs.

Martinez and Johnson's (2021) research highlighted the opportunities AI presents in expediting legal research and data analysis, ultimately improving case management and resource allocation. These analyses offer insights into the multifaceted impact of AI implementation, stressing the need for effective strategies to address challenges while capitalizing on opportunities to enhance legal efficiency and accessibility.

Sunley et al. (2021) highlights that city hosting highly successful International Financial Centers (IFCs), such as London, New York, and Hong Kong, have experienced significant increases in house prices and living costs. This observation aligns with Schumpeter's (1912/2017) theory, which posits that entrepreneurial profit stems from innovation and the resulting surplus over costs—often facilitated by new technologies, with money, credit, and finance playing crucial roles.

Johnson and Lee's (2020) research explored the use of AI in decision-making processes within the legal framework, highlighting

its ability to provide data-driven insights and enhance the accuracy of legal judgments. Their work, along with other studies, underscores the wide-ranging applications of AI in legal research, contract analysis, and decision-making, illustrating its potential to streamline and improve various critical aspects of the legal profession. Additionally, the literature consistently emphasizes the importance of ethical considerations and regulatory frameworks to ensure the responsible integration of AI within legal systems, reflecting ongoing discussions about the ethical implications of AI in the legal field.

Adams and Lee (2020) focused on the legal implications of AI integration, particularly in ensuring compliance with existing laws and regulations, especially in areas like data handling and information security. Their work contributes to a comprehensive understanding of the ethical responsibilities and legal obligations associated with AI adoption in legal systems, emphasizing the need for ethical guidelines and legal frameworks to govern AI practices and protect the integrity of the legal profession.

A thorough review of existing literature on AI's role in legal systems involves examining a wide array of scholarly articles, academic journals, and research papers. For example, **White and Smith's (2019)** study examined the practical applications of AI in automating legal tasks such as document analysis, drafting, and contract management. Similarly, research by Johnson et al. (2020) provided valuable insights into the effectiveness of AI-powered tools in facilitating case prediction and analysis, thereby streamlining decision-making processes within legal settings. These studies collectively contribute to a deeper understanding of the diverse ways AI is being integrated into legal practices, particularly its role in optimizing workflow efficiency and enhancing the quality of legal services.

Methodology

Research Design

This study adopts a qualitative research approach to explore the intersection of artificial intelligence (AI) and legal practice, specifically focusing on the future of legal services in the banking and financial sectors. The research is designed to gain an in-depth understanding of how AI is being integrated into legal services and its potential impact on these industries.

Data Collection

a. Literature Review

A comprehensive literature review will be conducted to analyze existing research on AI's role in legal practice, particularly within the banking and financial sectors. This includes scholarly articles, case studies, industry reports, and legal analyses published in academic journals, conference proceedings, and credible industry sources. The literature review will help identify key themes, trends, and gaps in the current understanding of AI's integration into legal services.

b. Case Studies

Case studies of law firms, financial institutions, and technology companies that have implemented AI in their legal practices will be analyzed. These case studies will focus on specific instances of AI applications in legal research, contract management, compliance monitoring, and risk assessment within the banking and financial sectors. The selected case studies will be analyzed for their implementation strategies, challenges faced, and outcomes achieved.

c. Expert Interviews

Semi-structured interviews will be conducted with legal professionals, AI specialists, and industry experts working at the intersection of AI and legal services in the banking and financial sectors. The interviews will aim to gather insights into the practical applications of AI, the challenges and opportunities it presents, and the ethical and regulatory considerations involved. The interviewees will be selected based on their expertise and experience in AI implementation and legal practice.

Data Analysis

a. Thematic Analysis

The data collected from the literature review, case studies, and expert interviews will be analyzed using thematic analysis. This involves coding the data to identify recurring themes, patterns, and relationships related to AI's role in legal services within the banking and financial sectors. The analysis will focus on understanding how AI is transforming legal practice, the benefits and risks associated with its use, and the future trajectory of AI in these industries.

b. Comparative Analysis

A comparative analysis will be conducted to evaluate the different approaches to AI integration in legal services across various organizations within the banking and financial sectors. This analysis will compare the effectiveness of AI applications, the challenges encountered, and the strategies employed to overcome them. The goal is to identify best practices and provide recommendations for successful AI adoption in legal practice.

Ethical Considerations

Given the sensitive nature of legal practice and the potential ethical implications of AI, this study will adhere to strict ethical standards. All data collected from interviews will be anonymized to protect the privacy of participants. Informed consent will be obtained from all interviewees, and the confidentiality of the information provided will be maintained. Additionally, the study will consider the ethical issues related to AI, such as bias, transparency, and accountability, and how these concerns are being addressed in the legal context.

Limitations

This study acknowledges certain limitations, including the reliance on qualitative data, which may not capture the full scope of AI's impact on legal practice. Additionally, the rapidly evolving nature of AI technology may result in findings that quickly become outdated. To mitigate these limitations, the study will focus on current and emerging trends and incorporate insights from a diverse range of sources.

Conclusion

The rapid integration of Artificial Intelligence (AI) into the legal profession, especially within the banking and financial sectors, is fundamentally transforming traditional legal services. This paper has explored the convergence of AI and legal practice, shedding light on how AI-driven technologies are revolutionizing key areas such as compliance, risk management, contract analysis, and dispute resolution. The research highlights both the opportunities and challenges posed by this technological shift, including ethical considerations and regulatory concerns.

As AI continues to evolve, legal professionals in the banking sector must adapt to new responsibilities in a technology-driven landscape. The intersection of AI and legal practice not only enhances efficiency

and accuracy but also redefines the role of legal practitioners, urging them to embrace innovation and continuous learning. The future of legal services in the banking and financial sectors will be shaped by the dual role of AI as both a catalyst for progress and a disruptor of traditional methods. This transformation presents a compelling case for legal professionals to integrate AI into their practice, ensuring they remain relevant and effective in an increasingly digital world.

Predictions: The Legal Function in 2025

- **Shift in Team Composition**: Half of the legal team may no longer be lawyers, with roles like paralegals, data analysts, and operational experts taking on more legal work.
- **Automation and Multidisciplinary Teams**: Increased use of automated legal solutions and chatbots, supported by a workforce with diverse skills.
- **CLM as Central Tool**: Contract lifecycle management (CLM) will be as integral to organizations as CRM and ERM, centralizing contract management to reduce costs and manage risks effectively.
- **Merging Legal Tech with General Tech**: Legal tech will integrate seamlessly into broader enterprise tech, with standalone legal solutions being replaced by holistic tech platforms.
- **Data-Driven Legal Work**: Reading and analyzing legal data will be as important as interpreting legal terms, helping legal teams identify opportunities to increase revenue and reduce risks.
- **Performance-Based KPIs**: Legal teams will be measured by KPIs that assess their contribution to the business's bottom line, focusing on both risk reduction and revenue generation.
- **Client-Centric Legal Services**: Legal delivery will become more user-centric, with internal clients expecting personalized, easy-to-use services.
- **Standardized Legal Work Automated**: Routine legal tasks will be automated and integrated into business processes, freeing up legal teams to focus on higher-value work.
- **Fully Digital Contracting**: Contracting processes will move entirely online, standardizing and speeding up negotiations, and enabling better risk management.
- **Cultural and Mindset Shift**: Successful transformation will

require significant cultural shifts, with legal teams needing new skills and strong change management.

- **Legal Chief Operations Officer (COO) Role**: The role of a Legal COO will rise in importance, complementing the General Counsel to ensure efficient and innovative legal service delivery.
- **Strategic Partnership**: By 2025, legal functions will transform into proactive, evidence-based partners to the business, focusing on adding strategic value.

Reference

- chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.iadclaw.org/assets/1/7/10.4-_Marchant-_ai_and_practice_of_law_SciTech_lawyer.pdf
- https://www.researchgate.net/publication/380508967_The_Impact_of_Artificial_Intelligence_on_Legal_Systems_Challenges_and_Opportunities
- https://emerj.com/ai-sector-overviews/ai-in-law-legal-practice-current-applications/
- https://www.transunion.co.uk/blog/emerging-financial-services-trends-and-the-future-of-banking#:~:text=The%20future%20of%20banking%3A%20Customer,expect%20from%20financial%20service%20providers.
- https://www.spotdraft.com/blog/ai-reshaping-lawyer-training?utm_term=&utm_campaign=Clickthrough+Leads-Performance+Max+Test+2&utm_source=adwords&utm_medium=ppc&hsa_acc=5694103801&hsa_cam=21463585418&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tgt=&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_

◆ ◆ ◆

16.

Privacy and Data Protection: A Human Rights Perspective

Dr Aneesh V Pillai & Nandana Rajesh***

Introduction

In the digital age, privacy and data protection are essential components of human rights. As technology develops, personal data is being collected and processed more and more frequently, which has led to worries about possible privacy violations.[1] This essay examines the complex interrelationships among privacy, data protection, and human rights, looking at the legal underpinnings of these ideas, their historical development, and the difficulties brought on by contemporary technological advancements. The study also addresses the significance of maintaining individual privacy while advancing technology, highlighting the necessity of strong legal frameworks and moral issues. Ultimately, it promotes a comprehensive strategy that guarantees the maintenance of privacy as a fundamental human right amidst changing digital environments.

1. S. Bedi, "The Essential Right to Privacy" (2021) 38(2) Harvard Human Rights Journal 245

***Coordinator, Justice V. R. Krishna Iyer Chair on Human Rights, School of Legal Studies, Cochin University of Science and Technology, Kerala.**

****Research Assistant, Justice V. R. Krishna Iyer Chair on Human Rights, School of Legal Studies, Cochin University of Science and Technology, Kerala.**

Background of the Study

The emergence of the digital age has revolutionized the gathering, analyzing, and sharing of information. Concerns over the security of personal information and privacy have grown in importance as technology has spread. The present study delves into the various aspects of privacy and data protection, emphasizing its inextricable link to human rights.

Objectives of the Study

1. To give a brief history of data protection and privacy.
2. To examine the legal systems in place for data protection and privacy.
3. To talk on how privacy rights are affected by technology progress.
4. To investigate the moral issues related to the gathering and use of data.
5. To make suggestions on how to protect privacy as an essential human right.

Historical Evolution of Privacy and Data Protection

The earliest human communities are where the concept of privacy originated, as people naturally desired to protect their private areas and personal data. People respected their houses and private matters in ancient Mesopotamia, Egypt, Greece, and Rome. As a result, these societies created unwritten norms of behavior to respect one another's privacy.[2] The idea of privacy has philosophical roots in ancient Greece, where philosophers such as Aristotle and Plato considered the concept of an individual's private domain. In his work "Politics," Aristotle recognized the value of both private and public life and the necessity for people to have private areas that are apart from the government. In a similar vein, the Roman notion of "domus" stressed the household's inviolability as a personal sanctuary.

The idea of privacy changed with societies, reflecting societal upheavals and modifications to cultural norms. The concept of confessional secrecy was first introduced by Judeo-Christian traditions, and the 1215 signing of the Magna Carta established the foundation for legal safeguards against unauthorized access. The significance of protecting personal information became increasingly apparent in the middle of the 20th century, especially in the years following World War

2. D. Solove, Understanding Privacy (Harvard University Press, Cambridge 2008)

II. The horrors of the conflict, especially the massive data collecting and monitoring carried out by authoritarian governments, highlighted the necessity of legal safeguards to stop abuses.

A significant turning point in the history of data protection was the 1948 adoption of the Universal Declaration of Human Rights (UDHR). The right to privacy is expressly recognized in Article 12 of the UDHR, which says that "no one shall be subjected to arbitrary interference with his privacy."[3] This paved the way for later advancements in data protection and established a fundamental concept for international human rights.[4] The first data protection regulations were created in the 1960s and 1970s in response to worries about the growing use of computers for processing and storing personal data. The Fair Credit Reporting Act (FCRA) was enacted in the US in 1970 with the intention of controlling how consumer credit information was used. Similarly, rules pertaining to the automated processing of personal data have been passed by European nations, most notably Germany and Sweden.

Established in 1980, the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines offered a set of guidelines for the preservation of privacy and served as a foundation for later international agreements. The significance of fair information practices which include the ideas of notice, consent, and data integrity was stressed by these standards. The first legally binding international agreement particularly addressing data privacy was the Council of Europe's 1981 adoption of Convention 108, often known as the Convention for the privacy of Individuals with respect to Automatic Processing of Personal Data. It created the idea of a data protection authority and outlined guidelines for the appropriate processing of personal data.

With the adoption of the Data Protection Directive in 1995, the European Union strengthened its commitment to data protection even more. The enactment of the General Data Protection Regulation (GDPR)[5] in 2018 was made possible by the foundation this directive created. Because of its extraterritorial reach, the GDPR constitutes a comprehensive legal framework that applies not only within the European Union but also globally.

In conclusion, the concept of data protection emerged as a separate legal idea following World War II, with international declarations and norms laying the groundwork for this development. As technology has

3. Universal Declaration of Human Rights (UDHR), Art. 12, 1948.

4. International Covenant on Civil and Political Rights (ICCPR), Art. 17, 1966.

5. General Data Protection Regulation (GDPR), European Union Regulation 2016/679

advanced, there has been a global dedication to safeguarding peoples' privacy, as evidenced by the ensuing growth of state legislation and international accords.

Legal Frameworks Governing Privacy and Data Protection

The groundwork for the acknowledgment of privacy as a fundamental human right is laid by important international documents including the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR). The international framework for the protection of privacy is further enhanced by regional agreements and treaties.

International Documents

- The Universal Declaration of Human Rights (UDHR): The Universal Declaration of Human Rights (UDHR), which was ratified by the UN General Assembly in 1948, is a key text outlining the fundamental rights to which every person is entitled. The right to privacy is expressly recognized in Article 12 of the UDHR, which says that "no one shall be subjected to arbitrary interference with his privacy." This recognition set a crucial stage for the global awareness of privacy as a fundamental human right.[6]

The acknowledgement of privacy in the UDHR is a reflection of the post-World War II determination to stop authoritarian state abuses, which included widespread monitoring and invasions of people's personal space. The pact influenced the creation of national laws all throughout the world and established a standard for later international agreements.

- The International Covenant on Civil and Political Rights (ICCPR): A significant international agreement that builds on the UDHR's tenets, the ICCPR was adopted by the UN General Assembly in 1966. The right to privacy is expressly enshrined in Article 17 of the ICCPR, which emphasizes the protection of people against arbitrary or illegal interference with their correspondence, family, home, or privacy. State parties are required by the ICCPR to guarantee the preservation of fundamental rights by means of laws and other measures.[7]

The UDHR and the ICCPR have been instrumental in making

6. Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/RES/217(III) (Dec. 10, 1948).

7. The International Covenant on Civil and Political Rights,1976

privacy a universally acknowledged human right. It guarantees that people have the ability to pursue compensation for infringements and offers a framework for countries to protect citizens' rights to privacy.

Regional Accords & Agreements

Regional conventions and accords, in addition to the UDHR and ICCPR, make a substantial contribution to the worldwide framework for privacy protection. Different regions have created specialized legislative instruments to handle these problems since they understand how important privacy and data protection are. The first legally binding international treaty addressing the protection of individuals concerning the automatic processing of personal data is the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108.[8] Adopted in 1981, it emphasizes the right of individuals to know and manage information about themselves and lays out guiding principles.

The right to privacy is recognized in Article 11 of the American Convention on Human Rights, commonly known as the Pact of San Jose, which applies to the Americas. This clause has been interpreted and applied by the Inter-American Court of Human Rights to shield people from unauthorized access to their personal information. Article 8 of the 1981-adopted African Charter on Human and Peoples' Rights covers privacy issues by highlighting the right to one's own space, residence, correspondence, and the preservation of one's honor and reputation.

By adapting the fundamentals to the unique requirements and environments of every location, these regional instruments add to the worldwide dialogue on privacy and data protection. Even though every instrument is different, they all aim to protect people's right to privacy within their particular legal frameworks.

The Information Technology Act, 2000

An important piece of law in India that covers a number of topics related to electronic commerce, electronic governance, and the use of electronic records is the Information Technology Act, 2000 (IT Act 2000). The IT Act includes rules pertaining to data protection and privacy in addition to its main goal of giving electronic transactions legal legitimacy. It's crucial to remember that the IT Act 2000 was passed before to the substantial technological breakthroughs and the extensive

8. Case of S and Marper v. United Kingdom, Application nos. 30562/04 and 30566/04, European Court of Human Rights, 2008

usage of the internet, thus it might not fully handle all current privacy and data protection issues.

Key Provisions of the IT Act 2000 related to Privacy and Data Protection

Section 43A - Compensation for failure to protect sensitive personal data: Section 43A: Restitution for Negligence in Safeguarding Sensitive Personal Information. This provision requires a body corporate (including businesses and other entities) to establish and uphold acceptable security standards and procedures if it owns, controls, or operates any computer resource that contains, handles, or deals with sensitive personal data. Should the body corporate fail to safeguard confidential information and cause unjustified profit or loss, it will be responsible for compensating the impacted individual.

Section 72A - Punishment for disclosure of information in breach of lawful contract: According to this clause, it is illegal to reveal information acquired while carrying out a legal contract without the subject's permission.

Section 69 - Power to issue directions for interception or monitoring or decryption of any information: Under certain conditions, especially those involving problems of national security, this section gives the government the authority to intercept, monitor, or decrypt any information created, sent, received, or stored in any computer resource.

Section 79 - Intermediaries not to be liable in certain cases: Although not directly linked to privacy, this clause shields online platforms, ISPs, and other intermediaries from liability for user-posted content as long as they follow specific due diligence guidelines.

Section 85 - Act to have an overriding effect: This section underlines that the IT Act 2000's provisions will take precedence over any conflicting laws.[9]

It's important to remember that, in contrast to more modern laws like the General Data Protection Regulation (GDPR) in the European Union, the IT Act 2000 does not offer a comprehensive framework for privacy and data protection. India has launched the Personal Data Protection Bill, 2019 (PDP Bill), which intends to offer a more strong and comprehensive legal framework for the protection of personal data, in response to the changing landscape of technology and data protection. When the PDP Bill is passed into law, it should close the gaps in the IT Act and bring India's data protection regulations into line

9. The Information Technology Act, 2000

with international norms.

International Cooperation and Collaboration

Given the worldwide scope of digital communication and data flows, effective international cooperation and collaboration are crucial to addressing privacy concerns. Cooperation between states is greatly aided by a number of organizations, including the United states, the Organization for Economic Co-operation and Development (OECD), and the International Conference of Data Protection and Privacy Commissioners (ICDPPC).

These organizations support the harmonization of privacy standards, the exchange of best practices, and the creation of a unified international framework for privacy protection. Furthermore, global partnerships aid in tackling new issues brought about by cross-border data flows, guaranteeing that privacy protection continues to be a common objective globally.

To sum up, important international agreements like the ICCPR and UDHR establish the basis for privacy as a basic human right. By addressing particular regional demands, regional conventions and treaties add to the global framework for privacy protection. The efficacy of privacy protections in a globalized environment is further enhanced by international cooperation and coordination, underscoring the significance of a uniform strategy for defending peoples' rights to privacy everywhere.

Technological Developments' Effect on Privacy Rights

- Analytics and Big Data: Large-scale personal data collecting and analysis have been made possible by the development of big data and advanced analytics. The consequences of big data for privacy are examined in this part, along with the difficulties presented by algorithmic decision-making and profiling.
- Internet of Things (IoT): As IoT devices proliferate, worries regarding the ongoing tracking and gathering of personal data are raised. The privacy issues of Internet of Things technology and the need for governmental measures are covered in this section.
- Machine learning and artificial intelligence (AI): Privacy is facing increasing issues as AI and machine learning are integrated into numerous industries. The study looks at the privacy issues

related to several technologies, including facial recognition and predictive analytics.

Ethical Considerations in Data Collection and Processing

- Informed Consent: One of the main tenets of moral data gathering is informed permission. In the digital age, getting meaningful consent can be difficult. This section examines alternate approaches that put the needs of users' understanding and control first.
- Transparency and Accountability: Two key components of ethical data management are guaranteeing transparency in data processing procedures and keeping organizations responsible for their deeds. The study looks at how accountability and openness contribute to preserving public confidence.
- Bias and Discrimination: Ethical questions are raised by the possibility of bias and discrimination in data-driven decision-making processes. The difficulties in reducing bias in algorithms and the moral ramifications of discriminating results are discussed in this section.

Recommendations for Preserving Privacy as a Fundamental Human Right

- Strengthening Legal Structures: In order to meet new issues in the digital age, the document promotes ongoing legal framework development and improvement. This entails revising current legislation and enacting fresh rules in line with emerging technology.
- Encouraging Ethical Data Management: Promoting ethical data practices within enterprises is essential to safeguarding privacy. In order to acquire, process, and store data responsibly, the document offers best practices and principles.
- Giving People More Control Over Their Personal Data: Giving people more control over their personal data is crucial. The significance of digital literacy, approachable privacy tools, and avenues for people to exercise their right to privacy are all covered in this section.
- International Cooperation: International cooperation is essential given the global nature of data flows. The necessity of international cooperation in establishing frameworks and standards for data protection and privacy is covered in the study.

Conclusion

Data security and privacy are not extravagances; rather, they are essential to personal freedom and dignity, especially in the modern digital era. This paper has offered a thorough examination of the development of these ideas across time, illuminating their philosophical roots, legal underpinnings, and difficulties brought on by the rapid advancement of technology. The concept of privacy has its roots in ancient societies, when people tried to create private areas that were off-limits to others. Over the years, philosophical influences, societal shifts, and legal advances have all worked together to establish privacy as a basic human right.

Concurrently, the mid-20th century saw the development of data protection as a separate legal concept in reaction to the growing dependence on technology and the necessity of protecting personal data in the wake of World War II. A strong international framework has been built to emphasize the value of privacy as an intrinsic human right, ranging from the UDHR and ICCPR to regional accords and conventions. The landscape of privacy and data protection has been significantly shaped by legal frameworks, both at the international and national levels. Tools like the GDPR have established norms that are embraced worldwide, impacting how organizations, governments, and people handle personal data.

The privacy protection landscape is always changing, though, and this poses new difficulties. Big data, the Internet of Things (IoT), and artificial intelligence (AI) have brought forth new complexity that call for a flexible and subtle approach. While there is no denying the advantages of technology breakthroughs, it is important to take into account the possibility that they may violate people's right to privacy. It takes a comprehensive strategy that goes beyond legal restrictions to strike a balance between the advantages of technology and the protection of privacy. Ensuring that data processing and gathering adhere to the values of accountability, transparency, and justice is contingent upon ethical considerations. In addition to legal and moral issues, striking this balance calls for international collaboration to standardize norms and procedures.

As society struggles to understand the complexities of the digital age, protecting privacy becomes critical to maintaining people's autonomy and sense of dignity. Privacy is a fundamental right that needs to be integrated into the development and application of technical

breakthroughs, not something that stands in the way of progress. Preserving privacy in the digital age requires a global commitment to ethical data practices, empowering individuals with control over their personal data, and increasing digital literacy.

In summary, the development of data protection and privacy is a reflection of the continuous effort to strike a balance between the advancement of technology and the defence of fundamental human rights. Although there are many obstacles to overcome, protecting privacy is still vital. A comprehensive and cooperative approach is necessary as we traverse the challenges of the digital age to guarantee that the advantages of technology strengthen rather than weaken the foundation of privacy that supports human dignity.

17.

Role of Social Media in Shaping Public Opinion in The Age of Ai: An Indian Perspective

Ramnik Bali & Arushi Khajuria***

Introduction

The rise of social media has fundamentally transformed the landscape of communication, information dissemination, and public opinion formation. Platforms like Facebook, Twitter, and Instagram have become essential tools for individuals to express their views, share information, and engage with others. In the AI age, where sophisticated algorithms and machine learning models drive content curation and recommendation, the impact of social media on public opinion has intensified. This article explores how social media shapes public opinion in the AI era, with a particular focus on Indian case laws and legal frameworks that address these dynamics.

Social Media and the Dynamics of Public Opinion

Social media platforms have democratized information dissemination, allowing individuals and groups to reach large audiences without traditional media intermediaries. The role of these platforms in shaping public opinion is multifaceted:

***Assistant Professor Dogra Law College.**

****Assistant Professor Dogra Law College.**

1. **Information Dissemination**: Social media enables rapid distribution of information, influencing how quickly and widely news and opinions spread. This immediacy can amplify both positive and negative messages, affecting public perception.
2. **Algorithmic Curation**: AI algorithms personalize content feeds based on user behavior, preferences, and interactions. This personalization can create echo chambers, where users are primarily exposed to information that reinforces their existing beliefs.
3. **Viral Phenomena**: Social media platforms are prone to the viral spread of content. Memes, hashtags, and viral posts can shape public discourse and influence collective opinions, often transcending traditional media channels.

The AI Era and its Impact on Public Opinion

The AI age has introduced advanced technologies that significantly impact how social media platforms operate and influence public opinion:

1. **Personalized Content Algorithms**: AI algorithms analyze user data to deliver personalized content. While this can enhance user experience, it can also lead to the amplification of extreme or misleading content. For instance, algorithms might prioritize sensationalist news over balanced reporting, skewing public perception.
2. **Deepfakes and Synthetic Media**: Advances in AI have enabled the creation of highly realistic but fake media, such as deepfakes. These can be used to spread misinformation or manipulate public opinion, posing significant challenges to the authenticity of information.
3. **Bots and Fake Accounts**: AI-driven bots and fake accounts can manipulate social media conversations, influence public opinion, and create false narratives. These artificial entities can sway elections, fuel social unrest, and distort public discourse.

Indian Case Laws Addressing Social Media and Public Opinion

In India, the intersection of social media, public opinion, and legal frameworks has been a subject of increasing scrutiny. Several landmark cases and legislative measures highlight the legal challenges and responses to the influence of social media:

1. **Shreya Singhal v. Union of India (2015)**: This landmark Supreme Court case struck down Section 66A of the Information Technology Act, 2000, which criminalized online speech deemed "offensive" or "annoying." The court ruled that the provision was unconstitutional due to its vague and broad language, which infringed on the right to freedom of speech and expression. This case marked a significant moment in the regulation of online content and highlighted the need for clear and precise legal standards.
2. **WhatsApp Privacy Policy Case (2021)**: The Delhi High Court addressed concerns related to WhatsApp's privacy policy changes and their impact on user data. The court examined whether the policy violated users' privacy rights under the Indian Constitution and relevant data protection laws. This case underscored the growing importance of data protection and privacy in the context of social media platforms.
3. **Tiktok Ban (2020)**: In response to national security concerns, the Indian government banned TikTok and several other Chinese apps. The ban was based on allegations of data privacy breaches and potential threats to national security. This move highlighted the intersection of national security, data privacy, and social media regulation.

Legal Frameworks Governing Social Media in India

India's legal framework for regulating social media and data protection includes several key laws and regulations:

1. **Information Technology Act, 2000 (IT Act)**: The IT Act provides a legal framework for electronic governance, cybercrimes, and electronic commerce. It includes provisions related to online content regulation, intermediary liability, and data protection.
2. **Data Protection Bill (2021)**: The Personal Data Protection Bill, 2021, aims to establish a comprehensive data protection regime in India. It addresses issues related to data processing, consent, and the rights of individuals concerning their personal data. The bill is a crucial step toward aligning India's data protection practices with global standards.
3. **Rules under the IT Act (2021)**: The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose stricter regulations on social media intermediaries. These rules require platforms to take down harmful content

promptly, appoint compliance officers, and adhere to guidelines for content moderation.

The Future of Social Media Regulation in India

As social media continues to evolve, so too will the legal and regulatory landscape. Key considerations for the future of social media regulation in India include:

1. **Balancing Regulation and Innovation**: Effective regulation must balance the need for public safety and data protection with the need to foster innovation and free expression. Overly restrictive measures could stifle technological advancements and limit the benefits of social media.
2. **Enhancing Transparency and Accountability**: Increased transparency in algorithmic decision-making and content moderation processes can help build trust between platforms and users. Ensuring accountability for the spread of misinformation and harmful content is crucial.
3. **Adapting to Emerging Technologies**: The rapid pace of technological advancement requires adaptive regulatory frameworks. Legislators and regulators must stay informed about new developments, such as AI-driven content creation and manipulation, to address emerging challenges effectively.

Conclusion

The role of social media in shaping public opinion in the AI age is profound and multifaceted. Social media platforms, driven by AI algorithms and advanced technologies, influence how information is disseminated, perceived, and acted upon. In India, legal frameworks and case laws address the complexities of this dynamic environment, balancing the need for regulation with the protection of fundamental rights.

As social media continues to evolve, ongoing dialogue and adaptive legal measures will be essential to navigating the challenges and opportunities of the digital age. By understanding and addressing these issues, India can better manage the impact of social media on public opinion while safeguarding democratic values and individual rights.

References

1. John Doe, *"The Future of AI in Education"* (Delhi: Education Press, 2024) 45
2. Chen, X., & Xie, H. (2023). *Adaptive Learning Technologies in Higher*

Education: A Review. Journal of Educational Technology Research, 15(3), 45-60.

3. Liu, Y., & Zhang, M. (2022). *Intelligent Tutoring Systems: Enhancing Learning with AI. International Journal of AI in Education*, 28(2), 97-112.
4. Johnson, L., & Brown, T. (2021). Leveraging Data Analytics in E-Learning Environments. Educational Data Mining Journal, 12(1), 23-39.Global Industry Analysis, "E-Learning Market in India to Reach $325 Billion by 2025" (accessed September 5, 2024) https://www.globalindustryanalysis.com/elearning-india.
5. Ibid.
6. Miguel A. Cardona, Roberto J. Rodriguez & Kristina Ishmael (2023). *Artificial Intelligence and the Future of Teaching and Learning*, Washington: U.S. Department of Education.
7. Mohsin Ali Khan (2023). Artificial intelligence in education: need of the hour. *Edutracks,* 22*(10),* 15-20.
8. Mudit Verma (2018). Artificial intelligence and its scope in different areas with special reference to the field of education. *International Journal of Advanced Educational Research*, 3*(1),* 05-10.
9. Neha Saini (2023). Artificial intelligence and its applications. *International Journal for Research Trends and Innovations*, 8*(4),* 356-360.
10. Patil, N.H., Patel, S.H. & Lawand, S.D. (2023). Artificial intelligence and its applications. *Journal of Advanced Zoology,* 44*(S-8),* 229-238.

◆ ◆ ◆

18.

Social Media Surveillance and Employment: Legal Issues in Monitoring Employee Behaviour

Poorvaja G, Shravit Arora** & Mini Srivastava****

Introduction

The legal position that regulates the practice of prospective employers in India to spy social media presence of workers can be discussed through a number of acts and constitutional provisions. A formidable legal restriction to surveillance activities is enshrined in right to privacy which is recognized as fundamental right under Indian Constitution through Article 21. In a historic judgement of *Justice K. S. Puttaswamy (Retd.) v Union*[1] of India the Supreme Court recognized this right and emphasized on the need of Right to Privacy even in workplace. Hence there is a need to ensure that while employees are being watched, their privacy is not infringed though the employer has the right to ensure that certain behaviours are correct and that certain standards are shown, the extent to which an employer goes in monitoring the workers should ensure that he or she covers the necessary and relevant grounds to achieve his or her intended goal.[2]

1. ibid

2. McDonald, Paula, and Paul Thompson. "Social media (tion) and the reshaping of public/ private boundaries in employment relations.", IJMR (69-84)

***Penultimate Law Student, Amity Law School, Noida.**

****Penultimate Law Student, Amity Law School, Noida.**

*****Assistant Professor, Amity Law School Noida.**

The amended Information Technology Act of 2000 forms a major foundation on which the acceptable limit of surveillance can be rendered. In as much as employers are legally allowed to access an employee's social media accounts or any personal data as an employee, the employer has to obtain prior consent from the affected employee especially if the information is of confidential nature. This particular mandate underlines how essential it is for companies to establish clear and specific guidelines concerning social media monitoring and ensure that their team members know what notion of monitoring the organization pursues.

Employers may also follow communications made in other open social media sites for the purpose of protecting their legal business interests but they can only do so legally. It has been said that any restrictions of the use of the social networking sites should be reasonable and necessary for the protection of the employer's business, for instance, where the employee might cause damage to the company's reputation, or where disclosure of certain information may be detrimental to the interest of that business. However, the use of information which in one way or the other has been procured in an illegal manner or random monitoring may have some legal consequences to employers, which may include invasions of the private rights of workers. Employers need to watch in adapting to new measures to fit with changes that continues to occur in regards to the regulation of privacy and surveillance of employees.

Digital Shadows: Employee Privacy amidst India's Social Networks

The right to privacy has rather gained significant recognition in India particularly in the social networks and at the workplace. The Indian Constitution conferred article 21 right of privacy by the judgement of Supreme Court in the case of Justice *K. S. Puttaswamy (Retd.) v. Union of India*.[3] This legislative provision of law states that workers shall be protected in exercising their right to privacy particularly on issues to do with their personal information and their activities on the social media. Employees may interpret this as their employers can monitor their conducts online and probably infringe on these rights because there is to this date no specific rule addressing the rights of employees to privacy at workplace.

3. Rathore, Shambhu Singh. "New dimension of right to privacy in social media ERA.", IJIRL, Volume III, Issue III, ISSN: 2583-0538, 2023

Employees' Sensitive personal data or information (SPDI) is somewhat protected under the Information Technology Act, 2000 and wrongs made under its enactment.[4] However, collection or processing of such data which entails private information that individuals post on the social media, requires authorization and only then can it be done. There is often lack of data protection laws, and because of this, the workers are subjected to invasive surveillance methods. There could be regulation that allows employers to read through the walls their employees are putting up on their social media accounts thus appearing as though there are conflicting civil liberties; the employer's right to protect the company's image and the employee's right to privacy.

Moreover even if the employees have liberty to post whatever they want on the social media then this liberty is not full liberty. Using social media during working hours may be restrained at a reasonable level which can be established by employers to maintain the courtesy and cover personal information. These limitations are also should be balanced against the four liberties of the employees: privacy and free speech included. This explains why it is important for organisations and employees to closely examine their rights given the fact that the laws surrounding the use of the internet in Kenya is bound to change especially with enactment of a comprehensive data protection law. Such policies should outline acceptable usage policies that address the rights of the employees and their privacy in the new world of advertising and public relations through social media. They should also ensure that the monitoring is done in an ethical and a more transparent manner.

Codes of the Digital Desk: Mapping India's Social Media Laws at Work

The Indian employers should develop extensive guidelines for employees' conduct on social media sites given the fact of social media monitoring and behaviour. Even though there is no law banning the use of social media at the work place, employers can refer to information technology act of 2000, private rights and employment laws. Casualization of these policies should ensure the regulation of the use of social media both within and outside working hours; ensure that the staff members understand how their behaviours shape their positions in the organization and the organization's image.[5] To avoid getting into

4. Patnaik, Ayushman, and Harshit Arora. "The Right to Privacy in the Digital Age: How Technology Is Impacting Privacy on Social Media.", IJIRL, Volume III Issue III | ISSN: 2583-0538

5. Kapoor, Kawaljeet Kaur, et al. "Advances in social media research: Past, present and future.", (2018), 531-558

numerous susceptibilities of the law, the employers should ensure that his policies do not infringe the labour laws in terms of freedom of speech and the right to privacy.

Ensuring that the organization lays down certain baseline of what type of conduct in the social media sites is acceptable and what is not, is among the prudent measures on how to observe the social media policy. Employers should block workers from using social media to bullying people, sharing sensitive company information or making inflammatory comments on their fellow employees or organization. The regulations should stress the importance of maintaining a clear line between one's work and personal life online and the staff should be advised to state on record that their opinions are not in any way reflective of the organizations[6]. Employers should also remind staff of guidelines to use when handling material or information which is considered by the staff to be potentially hazardous or risky and should encourage the staff to seek clarification about materials that they believe is not appropriate for online use.

Employers should also ensure that they have administrative measures through training programs to educate the staff members on specific matters affecting them such as the social media policy and the consequences involved. Employees that get trained feel well equipped to understand possible dangers of social media usage, and requisite of following set standards. Employers should also establish clear procedure for employees to lodge complaints violation of the social media policy and addressing of complaints regarding bad behaviour on social media platforms. Bosses may successfully negotiate challenges which the usage of social networks in business environment offers by protecting their interests and rights of their subordinates using themes of openness and responsible behaviour.

Silent Echoes: Social Media Surveillance and Speech in India

The laws concerning free speech of employees coupled with the monitoring of social media platforms in India is quite complex. While expected speech is protected by the constitution of the country, employers are at liberty to curtail the right of free speech. For example, the Information Technology Act of 2000 allows Indian companies to monitor employees' activities for various business benefits. However, due to this, the employees may never volunteer from offering their opinions

6. Satyanarayana, Pamarthi, Atchaiah Babu Undrakonda, And S. T. Naidu. " A Comparative Analysis Of International Standards And Indian Legal Provisions On Children's Privacy.", Jfcr, Vol. Ix, Issue-Ii, Book No.07, July – December: 2023 Issn: 2277-7067

as this is a result of surveillance, especially where issues concerning the workplace are involved. This relationship poses the equity between an employer's right to prevent compromise of his/her reputation as well as an employee's right to freedom of expression.

As seen in the recent court decisions from India, the companies have the liberty to set conduct rules, for example, regarding use of social media at work, but then they can deny their employees freedom of speech if their rules are overreaching. For instance, prohibited restraints may be challenged under the principles of NLRA, which protects employees' freedom to engage in integrated activities, if the employees use social media platforms to express their discontent or share experiences and/or information.[7] The matter is further compounded by the lack of specific legislation governing use of social media at the workplace that leaves the workers vulnerable to comp an action for expressing themselves on the internet. Apex courts have recognized that there is need to strike a balance by asserting that the policies must be reasonable, clear and not contradict employees' constitutional rights.

In addition, the consequences of monitoring extend beyond these examples and give consequences to the general culture of the workplace. Employees may keep quiet while having no capacity to discuss pertinent issues such as polices implemented at the workplace or the conduct of their superiors, since they may feel that their surfing habits are being closely monitored. Indeed, the employee morale may be dampened while creativity also tends to be suppressed in an atmosphere that is characterized by surveillance and an apparent disregard for the opinions of the employees. This means that employers have to ensure that they have policies that govern use of social media at workplaces but these has to adhere to international human rights law concerning workers and the reasonable business consideration as the laws are developed. Employers can also enhance the climate in many workplaces to counteract the potential threats of social media monitoring by listening to their employees' feedbacks.

Surveillance Morality: Unveiling Social Media Ethics in Indian Workspaces

Some of the implications arising from the practice include the following: The ethical issues arising from the social media monitoring practices are numerous and varied: The right balance

7. Mathew, Meera. "Freedom of information, right to express and social media in India.", IELR, Volume 3: Issue 2, 94–104

between the rights of workers and the companies' prerogative is not always easy to identify. While companies may argue that they monitor their employees' activity on social media with the intent of protecting their reputation, enforcing company policies, or preventing and preventing improper behaviour, is but unethical intrusion into employee rights to privacy and freedom of choice. Employees can perceive control over the utilization of their personal Twitter and Facebook accounts as encroachment on their privacy area since they have a expectation of privacy over them. According to the ethical standards, employers can expect this but at the same time they have to be free and transparent with the type and purpose of the monitoring activities.

Furthermore, there is an ethical question of the extent or the proportionality of such monitoring which directs attention to the relative size of the slice of businesses' social media monitoring responsibilities. The monitoring should be done to the extent that should meet the business necessity; any techniques, which make workers uncomfortable, should not be used. Namely, this may lead to the culture of employees mistrust and anxiety and is why employers have to be careful and not make their social media policies to vague and encompassing.[8] There should be well understood code of conduct that addresses acceptable behaviour standards on the net and on workers' right to freedom of speech and expression as pro-workers in matters concerning work related issues in particular. This balance is imperative to be aimed at establishment of the work culture that embraces freedom and individual responsibility.

Last but not least, potential impact of the monitoring procedures for the staff trust & morale is also an ethical consideration. The well-being and performance of the employees with regard to job happiness might decrease where they have the impression that they are constantly monitored. To avoid perceiving monitoring as an instrument of control, employers should make efforts in order to create conditions for monitoring that will be seen as a support and improvement tool. It is also in this level where workers can be engaged in a conversation regarding monitoring procedures and policies hence developing trust and ensuring that workers feel appreciated. It is possible to focus on

8. Indiparambil, Jijo James. "Privacy and beyond: Socio-ethical concerns of 'on-the-job'surveillance.", AJBE, (2019): 73-105

ethical issues in surveillance methods for a business to provide an acceptable and lawful working environment that respects the rights all the employees and fosters their free communication.

Web of Perils: Legal Traps in Social Media Surveillance for Indian Employers

The employers who try to monitor their staff members on social media in India take big risks legally. The contours of this area are defined by the Information Technology Act of 2000 which affirms the relevance of protection of personal sensitive data and privacy rights. Employers should, therefore, be careful especially when crossing the rights of the workers to privacy since it may lead to legal consequences. This includes using information collected without the consent of the dispenser of such information or even hacking into another person's social media profile. Besides possible fines a person may suffer civil consequences, such as demands for damages, violation of privacy rights can also attract attention of regulators, and it is notably that with India approaching the adoption of more comprehensive protection laws.

Moreover, there are more legal risks particularly on harassments and discrimination in as much as there is social media surveillance.[9] Employers have a need to maintain workplace free from harassment and discrimination and this includes harassment happening on social networking sites. Retaliation allegations may occur if a company monitors employees social media account and smears staff based on what they post on social networks. This is especially the case if the information being watched is involves talk of complaints at the workplace or whistleblowing. Ensuring that observation processes are open and fair is important for employers because Indian courts have stressed the importance of developing proper channels through which employees can report abuses without being penalized. Cyberspace crimes are subject to a variety of sanctions under the Information Technology Act, 2000 and it's implementing regulations. As per the provisions of Section 43 of Chapter IX of the Act, an individual who gains unauthorized access to the computer system, downloads data, introduces computer viruses, or causes denial of access may face a penalty of up to one crore rupees. Furthermore, according to Section 65 of Chapter XI, anyone who tampers with computer source documents and knowingly or intentionally conceals, destroys, or alters any computer source code, or incites another person to do so, faces a maximum sentence of three

9. Kumar, Deepak, and Prerna Singh. "Social media: new challenges for corporate governance.", IJR (2014): 343-352, Vol-1, Issue-4, May 2014 ISSN 2348-6848

years in prison, a maximum fine of two lakh rupees, or both.

Also, how employee rights are shifting in the digital age contributes to yet another legal issues tied to social media monitoring. This is why employers have to be careful not to infringe on the free speech of the employees because they are using the social media platforms more and more in expressing themselves. The use of contents generated on the social media to discipline employees has the potential of leading to defamation lawsuits or issues such as the incapabilities of disciplinary actions carried out by the employer. Some other prominent Indian Court case is *Tata Value Homes Ltd. v. Nityanand Sinha*[10] where the courts are even ready to protect the workers against unfair dismissal for voicing their opinions on social media.

Digital Filters: The Influence of Social Media on Hiring and Screening

This era has seen most employers in India turn to social media to background check the candidates and even draw their recruiting conclusion. From this point, the employer will be able to get to know the candidate's personality, favourite pastimes, and business demeanour much better than from the resumes and interviews.[11] Recruiters and employers can analyse a candidate's behaviour and conformity to working ethics, their communication skills and possibility to be a good fit for the company's environment by reviewing the applicant's social profiles. However, in a bid to avoid any negative effects of this technique, this creates more ethical and legal issues such issues including discrimination and privacy among respondents.

But if not well managed, the use of social media in the recruiting process is likely to lead to biases among businesses. Such personal attributes like age, gender, politics and religion among others could be revealed especially when revealing information on the social accounts. This information may then be used to make employment decisions and this results into discrimination litigation. Lack of proper regulation in employment of social media in India for recruitment means that firms will have to develop strict policies to ensure that their hiring process is gender-neutral. The probability of bias may be minimized, and it is possible to guarantee that only candidates who meet the necessary requirements and abilities are considered for a position, without regard to other factors such as personal traits which might become known due

10. Appeal (L) No.612 Of 2019, T.p.(C) No. 269/2016 Xvi-A

11. Vosen, Eva. "Social media screening and procedural justice: Towards fairer use of social media in selection.", ERRJ, (2021): 281-309, Volume 33

to the internet presence by setting specific rules for what information can be considered throughout the procedure of staff recruitment.

The legal pro Kerberos concerning the privacy rights in India also acknowledge the consent as the necessary precondition when Personal data shall be processed. By the Information Technology Act of 2000 and the Indian Constitution Article 21 freedom of privacy employers have to be transparent of their social media screening policies. If there is going to be scrutiny of the candidate's social media profiles at some stage of the recruitment process, perhaps, it is only reasonable to inform the candidate and if need be seek their permission. Hence, employers may use social media in their decisions in recruiting while at the same time protecting and respecting the rights of the candidates through giving ethical consideration their priority and the following regulations.

Conclusion

India's legal and ethical environment around social media monitoring and employment law is complicated and often changing. Social media's growing influence in both personal and professional domains has made it necessary to take a deeper look at where corporate monitoring ends and employee rights begin. Employers are required to carefully consider the necessity and proportionality of their monitoring activities because the right to privacy, as upheld by the Supreme Court in the Justice K.S. Puttaswamy (Retd.) v. Union of India case[12], serves as a crucial legal safeguard against invasive surveillance practices.

In India, employers have to balance upholding their employees' right to privacy and free speech with safeguarding their own legitimate economic interests. A legal foundation for controlling illegal access to social media accounts and sensitive personal data is provided by the Information Technology Act of 2000, which emphasizes the requirement for express authorization prior to any monitoring taking place. However, the absence of clear laws regulating social media use at work creates uncertainty and may expose workers to intrusive monitoring techniques.

One cannot ignore the moral ramifications of social media monitoring. Companies have to find a balance between the requirement to promote a transparent and trusting work atmosphere and their want to keep an eye on employee conduct. Overly permissive or unclear social media policies might discourage employees from being open and creative by

12. K.S. Puttaswamy (Retd.) v. Union of India case, Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1

creating a culture of fear and self-censorship. Employers must thus create social media policies that are equitable, comprehensible, and comply with law in order to safeguard the rights of their workforce as well as the organization's interests.

Social media surveillance carries substantial and complex legal issues. Employers who violate the law or participate in discriminatory or retaliatory behaviour risk severe legal repercussions, such as allegations of harassment, discrimination, and invasion of privacy. Employers must be aware of the changing legal landscape and modify their policies appropriately because of the possibility of defamation lawsuits and disagreements on the validity of disciplinary proceedings.

The legal issues surrounding social media surveillance in the workplace are probably going to get more complicated as India advances toward passing more extensive data protection legislation. Employers need to take the initiative to create and execute policies that not only adhere to current legal requirements but also foresee upcoming regulatory developments. Employers may successfully handle the challenges of social media surveillance while protecting their employees' rights and keeping a positive workplace culture by giving ethical issues top priority and creating an atmosphere of openness and accountability.

19.

Innovation to Encryption:Ai Innovation in Content and Privacy Challenges

Santushti Batta & Ms Mini Srivastava***

Introduction[1]

Artificial intelligence has fundamentally transformed the landscape of various industries and has had a principal effect on how we Homo sapiens have been using and interacting with technology. A.I analyse reader preferences and behaviour to tailor content in media engaging the audience and posting content consumption. It can crack marketing content by analysing highly personalised consumer data. Artificial intelligence enables visual search on e-commerce websites along with detailed description and reviews. Chat bots can handle customer grievances, streaming platforms use AI to analyse, viewing habits and AI can create immersive gaming experiences. Moreover, it in clinical documentation in the healthcare sector, it automates the creation of financial reports, summaries and provides insights into market trends, investment performance and financial statements. Generative models like chat GPT and Google is bad. Can generate humanistic

1. **Borda, Ann, et al. "Ethical issues in AI-enabled disease surveillance: Perspectives from global health."** *Applied Sciences* **12.8 (2022): 3890.**

***Student, Amity university, Noida.**

****Amity University, Noida**

text, visual art music and even video content.

In the process of connecting with AI, vast amount of personal data is required. Google and binge collect location data search queries platforms like Facebook and Instagram. Use AI to track user activity of and utilised for targeted advertising. Artificial intelligence driven recommendation systems, collect and analyse purchase history and customer feedback which can lead to privacy concerns. Ai tools analyse patient records and medical history for diagnostic purposes. It also poses a risk if sensitive health data is not adequately protected against breaches. Online shopping platforms use intelligence to manage customer data, including payment information and history. AI systems often operate as black boxes, making it difficult for users to understand how their data is being used or to provide consent. Even when data is anonymous algorithms. Can re-identify individuals by cross rectifying, aggregated data bases.

Thus, AI's impact on data privacy is multifaceted, presenting significant challenges across different industri[2]es and platforms. Addressing the sea where issues require robust data protection measures, transparency in AI operations and a commitment to ethical practises to safeguard personal information and maintain customer trust.

Data privacy concerns in the recent times

The convergence of AI and data privacy3 has become increasingly contentious and complicated as technological advancements become more ingrained in various aspects of our life and new privacy, concerns have emerged.

A number of imminent and popular data privacy concerns can be elaborated as following

Invasive Tracking

AI powered platforms, use, monitor user activity, biometrics, browser history and location data which can infringe on user privacy, if not carefully done or extent of data protection is not ensured

2. Galič, Maša, and Raphaël Gellert. "Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab." Computer Law & Security Review 40 (2021): 105486.

3. Onih, Valentine A., Yufenyuy S. Sevidzem, and Sulaimon Adeniji. "The Role of AI In Enhancing Threat Detection and Response in Cybersecurity Infrastructures." (2024).

Surveillance

Popular AI powered surveillance systems like facial recognition or being used for security purposes, which raises concerns about constant monitoring and potential miss use of data

Exposure Of Sensitive

Data breaches can lead to exposure of personal, financial and health related information which can be exploited for identity, theft, financial fraud or other malicious practices.

Unintended Consequences

Assistance handling, large data bases can sometimes in advertently expose data due to flaws, or loopholes in algorithms or their implementation

Opaque Data Practises

Users may not have a clear idea as to how the data is used or is being shared. The lack of transparency complicates the ability of the user to exercise control over data.

Re Identification

Ai algorithms can cross reference Anonymized or aggregated information with other data bases to re-identify individuals.This is essentially relevant when data is acquired from multiple sources.

Data Mining

A.I. can extr4act insights from large data bases that might inadvertently lead to identification of individuals

Bias Is In Ai Systems

If intelligence, algorithms or trained on the basis of story data which might contain of prejudices and viruses can produce discriminatory outcomes and lead to propagation of a conservative m[5]indset

---

4. Hartman-Caverly, Sarah, and Alexandria Chisholm. "Privacy literacy instruction practices in academic libraries: Past, present, and possibilities." IFLA journal 46.4 (2020): 305-327

5. Lichtenthaler, Ulrich. "Five maturity levels of managing AI: From isolated ignorance to integrated intelligence." Journal of Innovation Management 8.1 (2020): 39-50.

Regulatory Lap

Existing data protection laws do not adequately address the complexities of AI. Moreover, ethical considerations arise around the use of artificial intelligence in ways that may infringe pri6vacy.

Ownership Disputes

Determining who owns and controls data collection whether it is the user service provider or a third party can be a complex situation to tackle

Popular Scams

Deep Fake Scams

Deep fake is an advanced version of digital media manipulation in which AI and machine learning are utilised to create highly realistic, put fake audiovisual content by using extensive data sets to train a neural network to reassemble and recreate certain aspects of materials like facial features, voice or specific sequences. Also is capable of generating new content modelled on real humans.[7]

This raises significant security issues with regards to saving integrity of people along with data protection. It can fool biometric security and has opened a new dimension of threats in the area phishing. Victims have faced significant financial and psychological distress regarding the same.

AI generated deep fake blackmail. The fake technology has been used to create fake videos for blackmail and extortion whe[8]re individuals of falsely detected in compromising situation. Scammers used those videos to fabricate footage of individuals in illegal or embarrassing situation and threatened to release these videos unless the ransom was paid Victims faced financial losses and distress. As a result of the extortion, the realistic nature of these videos made it difficult for the victims to prove their authenticity and protect their reputation.

---

6. Galič, Maša, and Raphaël Gellert. "Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab." Computer Law & Security Review 40 (2021): 105486.

7. de Rancourt-Raymond, Audrey, and Nadia Smaili. "The unethical use of deepfakes." Journal of Financial Crime 30.4 (2023): 1066-1077.

8. Jones, Valencia A. Artificial intelligence enabled deepfake technology: The emergence of a new threat. MS thesis. Utica College, 2020.

Criminals have used AI-powered deep fake technology to create highly convincing voice replicas of executives or trusted individuals to conduct phishing scams. In one notable case, scammers used deep fake voice technology to impersonate the CEO of a company. The deep fake voice was us[9]ed to call a senior employee and instruct them to transfer a substantial sum of money to a fraudulent account. The scam resulted in significant financial losses for the company. The high fidelity of the voice replication made it challenging for the employee to distinguish the scam from a genuine request.

In 2018, California was one of the first state to pass a legislation regarding to sex with California consumer privacy act. In 2020, US introduced 'deep fake accountability act', which criminalises the same. A number of provisions in the IT act, 2000 in India, penalises Deepfake as it has become a huge threat, big enough to be taken into serious consideration.

Ai Powered Crypto Currency Fraud

Fraudsters have used AI driven chat bots to interact with potential investors offering higher returns on crypto currency investments, AI driven chat bots have fabricated success, stories and manipulated market data to your investors. Many people invested substantial amounts of money just to find out that investment platforms for fraudulent and promised returns that were non-existent. Regulatory bodies have a sensual heated surveillance on crypto currency platforms and AI driven financial services.

Major data breaches affecting global companies such as Equifax and Yahoo have led to the exposure of millions of records. Concerns about Chinese apps like TikTok's being used to collect user data and it potentially being shared with the Chinese government is a major cause of worry which also led the Indian government to ban 59 Chinese apps in India in June 2020 in European Union, GDPR mandates strict data protection measures and penalties for breach in the US CCPA provides residence of California with the rights to ac10cess and control their personal data.

Ai Driven Social Engineering Attacks

Intelligence tools have been employed in social engineering attacks, targeting financial institutions, where intelligence generated content

9. Kshetri, Nir. "The economics of deepfakes." Computer 56.8 (2023): 89-94.

10. Sabry, Farida, et al. "Cryptocurrencies and artificial intelligence: Challenges and opportunities." IEEE Access 8 (2020): 175840-175858.

is used to deceive employees into performing fraudulent actions. Attackers used AI to generate personalized messages and mails that emulated communication from senior executives or trusted contacts. These often include requests for sensitive information or unauthorized transactions, financial institutions experience, significant security, breach and financial losses as a result of successful social engineering attacks, the use of AI allowed for more convincing and targeted fishing attempts.

Ai Powered Fake Reviews and Ratings

Algorithms have been used to generate fake reviews and ratings to manipulate consumers behavior on e-commerce platforms. Scammers employed artificial intelligence to create large volumes of fake reviews and ratings for products and services. These reviews were designed to falsely post to the credibility of certa11in products or companies leading to skewed consumers perception who were misled into purchasing par products or services based on false information.

Automated identity fraud criminals have used AI to automate and scale identity theft operation. One case involves the use of AI to create synthetic identities and commit various types of fraud. Reason karatos were used to generate synthetic identities by combining real and fake personal information which was then used to open fraudulent accounts to apply for loans and engage in other forms of financial fraud. Identity theft led to significant financial losses and damaged credit scores for affected individuals. The automation of identity craft made it easier for criminals to operate on a larger scale.

Un's Approach to Ai Regulation

In a lot of countries activities across AI systems or subject to transversal regulations, they cater to personal data, protection and privacy, customer protection, economic competition, access to information and UN has recently adopted two key resolutions, A/RES/78/311, on 21st of March 2024 on taking up opportunities of trustworthy, AI systems, promoting sustainable development and the resolution is/are S/78/265 on 1 July 2024, on enhancing international cooperation on capacity building of AI. It elucidates upon regulatory approaches which the UN puts to play, motivating the artificial intelligence framework.

---

11. Sharma, Khushboo, and Niharika Maharshi. "Social Impacts of AI–Powered Online Reviews: An Ethical Consideration." Journal of Informatics Education and Research 4.3 (2024).

- ❖ Principal based approach offers a set of propositions that in lighten the path of developing AI systems through ethical and human rights. Promoting processes. OECD's 'Recommendation of council on AI 'is based on the same principle'.
- ❖ Standard based approach, assigns states regulatory powers to standard-setting entities that might be private publi[12]c or hybrid recital 121 of use artificial intelligence act expounds that 'Standardisation should play a key role to provide solutions in technical problems to providers to promote innovation with competitiveness.'
- ❖ Agile approach has been put to play to generate regulatory schemes in different sectors like finance and telecommunication
- ❖ Facilitating an enabling approach calls for responsible and ethical AI systems by private and public sectors like UNESCO. Do I look to Ram (readiness, assessment methodology) to evaluate if a country is prepared to implement Ai ethically.
- ❖ Adapting existing laws approach which chooses sector focused rules (health, education, agriculture etc) with transverse rules (criminal courts) instead of AI bills. Das, elaborating on current legal rules to include AI and emerging technology.
- ❖ Access to information and transparency is the most popular intelligence principal in A I bill worldwide.
- ❖ Risk-based approach prioritises measures according to assessment of risks that the parties will present to regulatory bodies Canada's directive on automate decision making which employs automated decision systems in a manner that it reduces risks to clients and federal institutions[13] is an example of the approach.
- ❖ Rights-based approach in shows to protect individual rights and freedoms, and establishes compulsory rules to guarantee the same
- ❖ Liability approach, assigns and sanctions the problematic uses of AI systems which aims at imposing mandatory standards of conduct backed by civil and criminal liabilities.

---

12. Salgado-Criado, Jesús, and Celia Fernández-Aller. "A wide human-rights approach to artificial intelligence regulation in Europe." IEEE Technology and Society Magazine 40.2 (2021): 55-65.

13. Fournier-Tombs, Eleonore. "Towards a United Nations internal regulation for artificial intelligence." Big Data & Society 8.2 (2021): 20539517211039493.

The United Nations and other international bodies have introduced several conventions and frameworks aimed at addressin[14]g AI-related crimes and cybersecurity challenges. While many of these conventions were initially designed to tackle broader issues of cybercrime and international security, they have increasingly incorporated aspects relevant to AI technology. Here's an overview of key conventions and frameworks relevant to AI-based crimes:

1. Budapest C[15]onvention on Cybercrime

Overview:

Full Name: Convention on Cybercrime

Adopted: November 8, 2001

Effective Date: July 1, 2004

Administered by: Council of Europe

Purpose:

The Budapest Convention is the first international treaty aimed at addressing cybercrime through harmonized legislation, international cooperation, and effective law enforcement. Provides a legal basis for combating cybercrime, which includes crimes facilitated by AI technologies such as hacking, fraud, and illegal interception.[16] cross-border cooperation among member states in investigating and prosecuting cybercrime, including those involving AI tools. Defines various cybercrimes and establishes standards for criminalizing offenses related to computer systems, data, and content.Provides mechanisms for international cooperation and mutual assistance in the investigation and p[17]rosecution of cybercrime.Ongoing updates and discussions to address emerging threats, including those related to AI, and to incorporate advancements in technology and cyber threats.

---

14. Ulnicane, Inga. "Artificial Intelligence in the European Union: Policy, ethics and regulation." The Routledge handbook of European integrations. Taylor & Francis, 2022.

15. Alic, Dalia. "The role of data protection and cybersecurity regulations in artificial intelligence global governance: a comparative analysis of the European Union, the United States, and China Regulatory Framework." Search in (2021).

16. de Almeida, Patricia Gomes Rêgo, Carlos Denner dos Santos, and Josivania Silva Farias. "Artificial intelligence regulation: a framework for governance." Ethics and Information Technology 23.3 (2021): 505-525.

17. Salgado-Criado, Jesús, and Celia Fernández-Aller. "A wide human-rights approach to artificial intelligence regulation in Europe." IEEE Technology and Society Magazine 40.2 (2021): 55-65.

2. UN Convention against Transnational Organized Crime (UNTOC)

Overview:

Full Name: United Nations Convention against Transnational Organized Crime

Adopted: November 15, 2000

Effective Date: September 29, 2003

Aims to combat transnational organized crime through enhanced international cooperation, mutual legal assistance, and the adoption of effective measures by member states.

While not specifically focused on AI, the Convention's provisions on organized crime can be applied to criminal activities facilitated by AI, including trafficking, fraud, and money laundering. Provides a framework for international cooperation in tackling sophisticated criminal operations that may involve AI technologies.Defines offenses related to organized crime and establishes measures for the investigation and prosecution of such crimes. Promotes international collaboration and assistance in the fight against organized crime.Discussions on updating the Convention to address new forms of organized crime, including those involving advanced technologies like AI.

3. The UN Convention on the Use of Electronic Communications in International Contracts

Overview:

Full Name: United Nations Convention on the Use of Electronic Communications in International Contracts

Adopted: November 23, 2005

Effective Date: March 1, 2013:

Facilitates international trade by ensuring that electronic communications, including those involving AI technologies, are recognized and legally enforceable in cross-border contracts. Addresses issues related to electronic communications and digital signatures, which are crucial for secure transactions involving AI technologies. Ensures that electronic transactions and communications involving AI are legally recognized and protected. Establishes the legal validity of

electronic communications 18and signatures.Provides mechanisms for resolving disputes arising from electronic contracts and communications. Efforts to align with technological advancements and address emerging challenges related to electronic communications and AI.

4. The UN Convention on the Rights of the Child (CRC)

Overview:

Full Name: Convention on the Rights of the Child

Adopted: November 20, 1989

Effective Date: September 2, 1990

Protects the rights of children and ensures their welfare and well-being in various contexts, including the digital environment.Protection from Exploitation: Addresses issues related to online exploitat19ion and abuse, including those involving AI technologies that may target children. Emphasizes the protection of children's privacy, which is crucial in the context of AI-driven data collection and surveillance. Protection from Abuse: Ensures protection from all forms of abuse, including online and AI-driven exploitation. Stipulates the need for safeguarding children's privacy and personal data.Ongoing discussions on enhancing protections for children in the digital age, including the implications of AI technology.

5. AI-Specific Frameworks and Initiatives

UNESCO's AI Ethics Framework

UNESCO has developed a global ethical framework for AI, focusing on ensuring that AI technologies are developed and used in ways that uphold human rights and ethical standards. Provides guidelines for the responsible use of AI and addresses issues related to misuse, including criminal activities.

The Global Partnership on AI (GPAI)

An initiative launched by vario[20]us countries and international

18. Gill, Amandeep S., and Stefan Germann. "Conceptual and normative approaches to AI governance for a global digital ecosystem supportive of the UN Sustainable Development Goals (SDGs)." AI and Ethics 2.2 (2022): 293-301.

19. Fiero, Anna Wright, and Elena Beier. "New global developments in data protection and privacy regulations: Comparative analysis of European Union, United States, and Russian legislation." Stan. J. Int'l L. 58 (2022): 151.

20. Shumailov, Ilia, et al. "UnUnlearning: Unlearning is not sufficient for content regulation in

organizations to support the responsible development and use of AI. Promotes collaboration on AI research and development, including efforts to prevent and address AI-related crimes.

Conclusion

Like two sides of a coin as artificial intelligence brings a plethora of advancements and efficient applications which continue to push the boundaries of what is possible and handle intensive tasks, it is also capable of exploitation of personal data for content generation, combined with increasingly sophisticated techniques like deepfakes and misinformation. It also underlines the dire need for robust privacy safeguards and regulatory measures. The synergy between human creativity and AI driven innovation is setting the playground for an president. It advancements in content creation, which, as a part of the process also calls for a collaborative approach involving policymakers, ethicist and technologists to check if a ice revolutionary potential is hornist responsibility with the imperative to shield individual privacy and prevent AI enabled crimes a proactive and comprehensive approach to prevent intelligence-based crimes by fostering interdisciplinary collaboration refining regulatory frameworks can mitigate the risks alon[21]g with relishing its unrivalled potential. Intelligence being one of the most prominent global advancements also gives a call for all the countries to unite on the global stage and come together to combat risks and exploitation, which might be as dangering or perhaps even more for a super developed nation, as or underdeveloped one.

advanced generative AI." arXiv preprint arXiv:2407.00106 (2024).

21. Hacker, Philipp, Andreas Engel, and Marco Mauer. "Regulating ChatGPT and other large generative AI models." Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency. 2023.

20.

Reshaping India's G20 Trajectory: Ai-Driven Sustainability In Waste Management

Shubhangi Agrawal, Daksh Tayal** & Daksh Tayal****

Introduction

Today, in the 21st century, sustainable development stands as s global necessity, addressing the the pressing need to balance social progress, environmental preservation, and economic growth. Within this intricate tapestry of global sustainability, India, being a prominent member of the G20, plays a crucial role. As one of the world's most populous and rapidly developing nations, India's actions has a large impact on the international stage, influencing not only its own trajectory but also the larger global pursuit of sustainable growth. This significance arises from the G20's recognition of the necessity for cooperative efforts to address environmental challenges and combat climate change, as well as to promote the shift to more flexible, transparent, and ecologically friendly energy systems, is what gives this significance.[1]

At the heart of this pursuit lies the indispensable role of technology and innovation. Among the multifaceted tools available, Out of the

1. **"Sustainability - Climate Sustainability and Energy", available at: https://www.oecd.org/g20/topics/climate-sustainability-and-energy/**

***(Penultimate Student) Amity Law School, Noida.**

****(Penultimate Student) Amity Law School, Noida.**

***** (Penultimate Student) Amity Law School, Noida.**

number of tools that are available at our disposal, Artificial Intelligence (AI) emerges as a game-changer, with the ability to revolutionise a number of industries. In particular, the integration of AI into sustainable waste management practices is of utmost importance. Waste management represents a common issue where economic, environmental, and social concerns converge. It is not merely a matter of discarding refuse but rather a complex web of issues including resource conservation, pollution mitigation, and public health.

In this context, AI-powered sustainability stands out setting a ray of of hope, offering innovative solutions to age-old problems. AI's capacity to analyze vast datasets, optimize resource allocation, and predict environmental trends revolutionizes waste management strategies. Thus, by implementing these intelligent systems, we can enhance waste collection efficiency, minimize landfill usage, reduce pollution levels, and ultimately creating more resilient and eco-friendly communities.

Therefore, the focus of the study is to explore the far reaching effects of AI-powered sustainability within India's waste management strategy. It examines how this synergy can not only elevate India's environmental resilience but also strengthen its position within the G20. As we delve into this dynamic space where technology meets sustainability, we uncover the the opportunities, difficulties, and promises that lie ahead for India as a G20 member and the crucial role that it can play in paving the way for a more sustainable future for all of us.

India's Waste Management Landscape

India is a country which is known to be standing as one of the world's most populous nations and experiencing rapid urbanization, because of which it often finds itself tangled in a complex web of waste management challenges and opportunities. Annually, the nation generates an astonishing 62 million tonnes of municipal solid waste, a figure that keeps rising due to the country's burgeoning urban centers and expanding population.[2]

Within this landscape, India employs a variety of waste management practices, which, although varied, often fall short of addressing the ever-mounting waste generation. In urban areas, municipalities often utilize formal waste management systems for processes like collection,

2. Bindu Gopal Rao, "What do we do with India's mounting waste problem?" available at https://www.fairplanet.org/editors-pick/india-waste-problem/#:~:text=The%20country's%20population%20generates%2062,165%20million%20tonnes%20by%202030

transportation, and disposal of waste, the end point of which is designated landfills. However, the efficiency and reach of these systems significantly differ across regions, with smaller municipalities and rural areas frequently often struggling with issues like poor infrastructure and irregular garbage collection.

Nevertheless, a major issue continues to be the large amount of waste that remains either uncollected or dumped in makeshift sites especially in underprivileged areas. In such places open dumping and the careless burning of waste become common practices. While these methods are efficient they come with a heavy price. They significantly contribute to pollution by releasing harmful gases into the air and posing serious health risks to nearby communities. Thus it is essential to acknowledge the unsung heroes of India's waste management system the informal waste pickers who navigate through challenges to recover materials. However, their commendable efforts often take place under conditions marked by job security and limited access to social protections.

Moreover, the consequences of India's waste management are felt on both an ecological level as well as an economic level. Environmental challenges include the issue of soil and water contamination, characterized by the toxic leachate that seeps from landfills, as well as the hazardous air quality resulting from open waste burning. The country's contribution to greenhouse gas emissions is further worsened by methane emissions from organic waste that is decomposing in landfills. The economic repercussions are equally troubling; India misses out on potential revenue and employment prospects, in the growing recycling sector as well as valuable materials that could be recycled for profit.

In light of all these complexities there is an urgent need to prioritize waste management issues as a key element of India's journey towards sustainable growth. Effective waste management goes beyond simply getting rid of waste; it also involves conserving resources, minimizing pollution and enhancing public health. By strengthening its waste management systems and practices India can reduce environmental damage, conserve valuable resources and provide its citizens with a healthier and more sustainable future. Moreover, by aligning these efforts with global sustainability objectives India can position itself as a proactive and responsible player in international platforms like the G20 where discussions on environmental responsibility and economic progress revolve around sustainability. Amidst the challenges India faces in its waste management landscape lies a significant opportunity

to harness waste management capabilities for both local advancements and substantial contributions to global sustainability initiatives.

Application of AI in Waste Management

In today's time, Artificial Intelligence AI is leading a significant change as to how we handle waste management providing a solution to tackle the various challenges tied to issues like waste collection, recycling, pollution control, energy generation, and operational efficiency. Within this transformative landscape, AI-driven techniques such as smart bins, fleet management, pollution monitoring, waste-to-energy processes, predictive analytics, and optimization are poised to revolutionize waste management practices, forging a path toward sustainability, efficiency, and environmental responsibility. In this discourse, we delve into these pioneering AI-driven technologies and their contributions to a cleaner, greener future.[3]

1. **Smart bins**, that represents a cornerstone of AI's influence in waste management, are equipped with sensors and real-time data collection capabilities.[4] These intelligent containers continuously monitor their fill levels and communicating this information to a central system. This data is analysed by AI systems to forecast when a bin will fill up. Such predictive capabilities often help in optimizing waste collection routes, deploying trucks only when bins are nearing fullness. This not only minimizes operational costs but also substantially reduces the environmental impact of waste collection, as fewer unnecessary pickups mean fewer emissions and less fuel consumption.
2. **AI-driven fleet management** further amplifies the optimization of waste collection processes thereby, drawing data from various sources like smart bins, GPS, and real-time traffic conditions, AI algorithms help to calculate the most efficient routes for waste collection vehicles. This dynamic route optimization significantly reduces fuel consumption, minimizes travel time, and results in substantial cost savings. By ensuring that trucks are dispatched precisely when required, AI contributes significantly to the overall sustainability of waste management practices.[5]

3. Sanksshep Mahendra, "Artificial Intelligence in Waste Management" Artificial Intelligence+, 2023, available at: https://www.aiplusinfo.com/blog/artificial-intelligence-in-waste-management/.management**. (last visited September 8, 2024).**

4. "Artificial Intelligence and Waste Management," RTS. available at: https://www.rts.com/blog/ai-and-waste-management/

5. "How to utilize from AI in waste management," Evreka, 2022, available at: https://evreka.co/blog/how-to-utilize-from-ai-in-waste-management **(last visited September 8, 2024).**

3. AI's utility extends to **pollution monitoring and control** in waste management. AI-driven systems analyze data from sensors and surveillance cameras to detect illegal dumping or open burning of waste. Early detection empowers swift responses and regulatory enforcement, effectively curbing environmentally harmful activities. Additionally, AI plays a pivotal role in monitoring and mitigating environmental risks tied to landfills, such as leachate and gas emissions. These real-time interventions safeguard ecosystems and public health, aligning waste management practices with broader environmental sustainability objectives.
4. **Waste-to-energy processes** benefit immensely from AI's optimization capabilities. AI algorithms fine-tune the incineration of non-recyclable waste to maximize energy generation while minimizing emissions. This optimization not only reduces waste volume but also contributes to the generation of clean and sustainable energy, addressing both waste reduction and clean energy production goals.
5. **Predictive analytics**, an essential AI component, offers invaluable insights into waste generation patterns. By scrutinizing historical data and real-time information, predictive models anticipate fluctuations in waste generation.[6] For instance, during holidays or special events, waste generation often experiences a notable uptick. AI's predictive capabilities forecast these patterns, enabling efficient resource allocation. As a result, waste management operations remain agile and responsive to evolving conditions, bolstering efficiency and resource utilization.

Thus, AI's role in waste management is comprehensive, encapsulating smart bins for optimized collection, AI-driven fleet management, pollution monitoring and control, enhanced waste-to-energy processes, predictive analytics for adaptable resource allocation, and advanced recycling sorting techniques. These AI-powered innovations are reshaping waste management practices, making them not only more efficient and cost-effective but also more environmentally sustainable. As the waste management sector aligns itself with broader sustainability goals, AI emerges as a pivotal tool in crafting a cleaner, greener, and more efficient future.

---

6. "How AI is Revolutionizing Solid Waste Management,." available at: https://swana.org/news/blog/swana-post/swana-blog/2023/12/11/how-ai-is-revolutionizing-solid-waste-management

Linking AI Driven-Waste Management to Environmental Resilience In India

India, home to over a billion people and undergoing rapid urbanization, faces a formidable waste management challenge. Against this backdrop, the integration of Artificial Intelligence (AI) into waste management practices assumes immense importance. AI not only helps alleviate the environmental strains resulting from waste but also aligns with India's sustainability goals.

At the heart of AI's role in India's waste management lies the optimization of waste collection. Mumbai, one of India's bustling metropolises, provides a prime example. The city deploys AI-powered sensors in waste bins to monitor fill levels in real-time. When a bin nears capacity, the system triggers waste collection, optimizing route planning and minimizing unnecessary trips. This not only saves operational costs but also substantially reduces the carbon footprint, aligning with India's aspirations for cleaner urban environments.[7]

Recycling, a key facet of waste management, also benefits from AI. Bengaluru, known as the Silicon Valley of India, employs AI-driven recycling technologies to address its growing waste woes. These systems employ computer vision to distinguish between different materials in waste streams, enhancing recycling accuracy.[8] By diverting materials from landfills and channeling them back into the production cycle, these technologies play a pivotal role in resource conservation, a crucial element of India's sustainability agenda.

Pollution control and monitoring are paramount in India, where air and water pollution often reach critical levels. New Delhi, the nation's capital, grapples with severe air pollution issues. AI-driven pollution monitoring systems analyze data from various sources, including industrial emissions and traffic patterns, to generate real-time pollution maps.[9] This data empowers policymakers to enforce targeted measures to reduce pollution levels. Additionally, AI-based monitoring of water bodies, such as the Ganges River, helps in early detection of contaminants, safeguarding the health of millions who depend on these water sources.

---

7. Murshid Reza, "AI-Driven Solutions for Enhanced Waste Management and Recycling in Urban Areas", 8 IJSICS (2023).

8."Bengaluru: Digital Mapping to Manage Solid Waste – Global Opportunity Explorer,." available at: https://goexplorer.org/bengaluru-digital-mapping-to-manage-solid-waste/

9. "Drones and AI tools to help tackle Delhi pollution," (2022). available at:https://indianexpress.com/article/cities/delhi/new-delhi-pollution-projects-caqm-drones-ai-8262153/

AI's role in waste-to-energy processes significantly contributes to India's resilience against energy challenges. In cities like Pune, waste-to-energy plants leverage AI to optimize combustion processes, improving energy generation efficiency and reducing emissions. This aligns with India's ambitious renewable energy targets and bolsters its ability to manage energy resources sustainably. Furthermore, Delhi's innovative "Waste to Wonder Park," which features replicas of iconic world landmarks constructed from scrap materials, exemplifies AI-driven creativity in waste management. AI technologies assist in sourcing suitable materials, optimizing construction processes, and even predicting visitor traffic to ensure the park's efficient operation.

Therefore, the integration of AI in waste management in India is a multifaceted approach that enhances environmental resilience while aligning with the nation's sustainability goals. Through optimization, recycling enhancement, pollution control, and sustainable energy generation, AI empowers India to address its unique waste management challenges effectively. These AI-driven solutions, along with innovative projects like Delhi's "Waste to Wonder Park," serve as a testament to the transformative potential of technology in propelling India toward a sustainable and environmentally resilient future.

The G20 and Sustainable Developmental Goals: India's Waste Management Strategy

The Group of Twenty (G20) brings together some of the world's most influential economies, each with its unique set of economic and environmental challenges. Amid the increasing global focus on sustainability and the United Nations Sustainable Development Goals (SDGs), India's approach to waste management offers a compelling case study, showcasing how a nation's strategy can be intricately tied to these global objectives.

India's waste management landscape has evolved significantly in response to its population growth and urbanization. These developments align closely with SDG 11, "Sustainable Cities and Communities," which emphasizes the need for inclusive, safe, and sustainable urban areas. India's investment in AI-driven waste management technologies, particularly in its urban centers, exemplifies its commitment to creating more efficient, cleaner, and sustainable cities. These technologies optimize waste collection, reducing the environmental footprint of urban areas, and thus contributing to achieving SDG 11.

Furthermore, India's waste management strategy has a direct bearing on SDG 12, "Responsible Consumption and Production." A core tenet of this goal is to substantially reduce waste generation. India's adoption of AI-driven recycling and resource recovery processes plays a pivotal role in achieving this target. These innovations promote responsible consumption by reducing waste and recycling valuable materials. Consequently, India is contributing to more sustainable production and consumption patterns, in line with SDG 12.

India's focus on waste-to-energy processes, particularly those enhanced by AI, is instrumental in addressing climate change, as outlined in SDG 13, "Climate Action." By efficiently converting non-recyclable waste into clean energy, India curtails emissions from landfills and incineration. This aligns directly with SDG 13's call for urgent global action to combat climate change and its impacts. AI-optimized waste-to-energy processes represent a sustainable approach to energy generation while mitigating climate-related risks.

Lastly, India's approach to waste management underscores the significance of international collaboration, echoing the essence of SDG 17, "Partnerships for the Goals." India's adoption of AI-powered waste management technologies often involves partnerships with international organizations and technology providers. This highlights the importance of global cooperation in seeking innovative solutions to common challenges. Such partnerships facilitate knowledge exchange, technology transfer, and the sharing of best practices, all of which are fundamental to achieving the SDGs.

Thus, India's waste management strategy offers a compelling example of how G20 nations can align their initiatives with the SDGs. Through AI-driven waste management innovations, India contributes to SDG 11, SDG 12, SDG 13, and SDG 17[10]. These efforts underscore the pivotal role of sustainable waste management in achieving broader sustainability and environmental resilience goals on both the national and international stages.

Enhancing India's G20 Position Through AI-Driven Sustainability

India's role within the G20 presents a unique opportunity for the nation to amplify its influence on the world stage and advocate for sustainable development. In recent years, India has been exploring avenues to strengthen its standing and make substantial contributions to the G20 agenda. One such avenue lies in harnessing the transformative

10. "THE 17 GOALS | Sustainable Development", available at: https://sdgs.un.org/goals

power of artificial intelligence (AI) to drive sustainability within the realm of waste management. India faces formidable challenges in waste management, owing to its rapid urbanization and population growth. Conventional waste management systems have struggled to keep pace with the escalating waste generation, leading to adverse environmental impacts and public health concerns. Recognizing the urgency of addressing these issues, India has embarked on a journey towards innovative waste management practices, and AI has emerged as a crucial enabler. AI encompasses a wide range of technologies, including data analytics, machine learning, and the Internet of Things (IoT). When applied to waste management, these technologies enable real-time data collection, predictive analytics, and optimized resource allocation. Machine learning algorithms can predict when equipment maintenance is required, reducing downtime. These advancements yield a more efficient and streamlined waste management process. AI-driven waste management practices also allow for better tracking and monitoring of waste flows, enabling authorities to make informed decisions and respond promptly to emerging challenges. This real-time data-driven approach enhances the overall efficiency of waste management processes.[11]

One of the most compelling aspects of AI-driven sustainability in waste management is its potential for generating substantial economic benefits. By optimizing waste collection and recycling processes, AI reduces operational costs for waste management companies. Furthermore, it fosters the creation of green jobs in technology-driven sectors and the monetization of recyclables and waste-derived energy, stimulating local economies. AI-driven waste management also aligns with the promotion of a circular economy. Through advanced sorting and recycling processes, waste materials can be efficiently repurposed and reintroduced into the production cycle. This not only conserves resources but also reduces the need for costly landfill disposal. Such economic efficiency resonates with the G20's objective of promoting inclusive economic growth.[12]

AI-powered sustainability in waste management contributes significantly to environmental progress as well. The reduction of landfill use decreased air and water pollution, and lowered carbon

11. Shipra Sinha, "Innovation, Sustainability, and AI – SAP in India" CMR India, 2023, available at: https://cmrindia.com/innovation-sustainability-and-ai-sap-in-india/ (last visited September 8, 2024).

12. Abhishek Ahuja et al., "Driving Sustainable and Inclusive Growth in G20 Economies", McKinsey & Company (2023). available at: https://www.mckinsey.com/in/our-insights/driving-sustainable-and-inclusive-growth-in-g20-economies**.**

emissions are direct outcomes of these practices. AI helps identify recycling opportunities, optimize waste-to-energy conversion, and minimize the environmental impact of waste disposal. India's commitment to addressing these environmental challenges through AI-driven sustainability aligns with the G20's environmental priorities. In an era marked by climate change and environmental degradation, India's proactive stance positions it as a leader in sustainable waste management, enhancing its standing in discussions related to global environmental stewardship within the G20.[13]

Beyond economic and environmental benefits, AI-driven sustainability in waste management results in significant societal improvements. Cleaner and healthier living environments lead to an improved quality of life for India's citizens. Additionally, the creation of green jobs in waste management and technology sectors contributes to poverty reduction and social development, aligning with the G20's goal of inclusive growth and social welfare. AI-driven sustainability ensures that the benefits of economic growth are distributed more equitably across society.

India's embrace of AI-driven sustainability in waste management offers a multifaceted path to strengthen its position within the G20. The economic advantages, environmental progress, and societal improvements stemming from these initiatives closely align with the G20's core objectives. As India pioneers innovative solutions to waste management challenges, it not only underscores its commitment to sustainability but also meaningfully contributes to global efforts aimed at forging a more sustainable and prosperous future for all. This comprehensive approach reflects India's proactive stance in shaping the G20's agenda and showcases its potential as a leader in sustainable development on the global stage.

Challenges and Future Directions

AI-driven waste management has the potential to revolutionize how societies handle waste, promoting sustainability and responsible environmental stewardship. However, several challenges must be addressed, including data quality and availability, cost barriers, integration issues, technological limitations, and regulatory concerns. Looking ahead, promising future directions can further enhance AI-driven waste management.

13. Ritu Verma, "G20 and Sustainable Development," 6 IJFMR (2024).

One of the primary challenges in AI-driven waste management is the quality and availability of data. Effective AI algorithms require large and diverse datasets, but many regions, especially in developing countries, lack comprehensive data on waste generation, composition, and disposal. Inconsistent and unreliable data collection methods hinder waste management optimization. Accurate and timely data collection is crucial for future developments in this field. Cost is a significant challenge in implementing AI-driven waste management systems.[14] The initial investment can be a barrier, especially for resource-constrained municipalities. Costs include hardware, sensors, AI software, and personnel training. Reducing these costs is pivotal for widespread adoption and equitable implementation. Integrating AI into existing waste management infrastructure is complex. Many cities have established systems that may not be compatible with AI-driven solutions. Retrofitting or upgrading these systems can be costly and logistically challenging. Compatibility issues and seamless integration must be addressed to ensure AI enhances existing processes. Technological infrastructure limitations are obstacles, particularly in regions with inadequate resources. Smaller communities may lack funding and expertise to leverage AI innovations. Issues like unreliable internet connectivity and power supply hinder AI-powered waste management solutions. Addressing these challenges is essential for inclusivity in sustainable waste management.[15]

The future of AI-driven waste management holds promising directions. Waste sorting and recycling will improve with AI-powered robotics and sorting machines, boosting recycling rates and resource recovery. Real-time monitoring and predictive analytics will optimize waste collection routes, reducing unnecessary pickups and resource wastage. Integration with the Internet of Things (IoT) will lead to smart waste bins with sensors, streamlining data collection and waste collection processes.[16] AI-driven waste management will promote a circular economy by encouraging reuse, remanufacturing, and recycling through intelligent solutions. Personalized feedback and incentives will engage consumers in responsible waste management. AI will assess the environmental impact of waste management processes, optimize routes to reduce emissions, and ensure the sustainability of waste-to-energy solutions. In landfill management, AI will monitor and mitigate issues

14. Gurmehar Kaur and Arvind Dhingra, "*Use of Artificial Intelligence for Waste Management", IJLTEMAS* **(2023)**

15. Maryam Abbasi and Ali El Hanandeh, "Forecasting municipal solid waste generation using artificial intelligence modelling approaches," 56 Waste Management 13–22 (2016).

16.Supre note 12.

like leaks, gas emissions, and soil contamination. Global collaboration and data sharing will foster the exchange of data and best practices. Regulatory frameworks specific to AI-driven waste management will ensure data privacy, security, and ethical use. Continuous research and innovation will drive new waste management technologies, while public awareness and education campaigns will promote responsible waste reduction and recycling practices.[17]

AI-driven waste management has the potential to create a more sustainable and efficient waste management system. Addressing challenges related to data, cost, integration, infrastructure, and regulation is essential. Embracing promising directions like improved recycling, real-time monitoring, and IoT integration can lead to a cleaner and more sustainable future for all.

Conclusion

Artificial intelligence (AI) has emerged as a powerful catalyst in propelling sustainable waste management practices towards a future marked by unprecedented efficiency and heightened environmental awareness. Within India, where waste management challenges are magnified by rapid urbanization and a burgeoning population, AI-driven solutions offer a beacon of promise. These innovations seamlessly align with Prime Minister Narendra Modi's Swachh Bharat Abhiyan (Clean India Campaign), ushering in the prospect of cleaner and more sustainable urban environments.

At the heart of sustainable waste management lies the 3R framework – reduce, reuse, and recycle – and AI acts as a formidable ally in upholding these principles. By curtailing waste generation at the source, optimizing resource utilization, and advocating circular economy practices, AI significantly complements these sustainability tenets. Although hurdles such as technological maturity, cybersecurity concerns, and initial capital outlays loom, the potential benefits far outweigh these challenges.

From the vantage point of India's commitment to sustainability within the G20, the integration of AI into waste management perfectly aligns with the nation's vision. India's steadfast emphasis on sustainability, innovation, and international collaboration resonates harmoniously with AI's transformative potential in waste management. The recent allocation of approximately USD 19 billion to the Swachh

17. Puneet Sharma and Upma Vaid, "Emerging role of artificial intelligence in waste management practices," 889 Waste Management (2021).

Bharat Mission in the Union Budget is a testament to India's resolute commitment to advancing clean and sustainable waste management practices. Scientific segregation of waste, granted prime importance, forms a cornerstone of this endeavor, with new-age AI solutions poised to play a pivotal role in creating the necessary infrastructure.

This forward-looking approach not only aligns with India's pursuit of a Swachh Bharat but also strengthens its dedication to broader sustainability objectives. By leveraging AI's transformative capabilities, India is on the brink of achieving cleaner cities, reduced environmental impact, and improved public health. As India takes strides towards a more sustainable and environmentally resilient future, AI stands as an indispensable tool, embodying the nation's vision for a cleaner, greener tomorrow.

◆ ◆ ◆

21.

Taming the Giant – Analyzing the Potential Possibilities of Inclusion of Artificial Intelligence in The Judiciary

*A.Anchirppa**

Introduction

Modern era has blended so much with internet that it plays a major role in all areas including health, education, nutrition, well-being etc. Kepios (a private limited company that studies digital behaviour) analysis indicates that internet users in India increased by 34 million (+5.4 percent) between 2021 and 2022.[1] Other technical terms like machine learning or deep neural networks or artificial intelligence are already blended into our day-to-day activities like booking a cab or auto, using an online map or online shopping etc. These technologies are also used in governance aspects more pertaining to criminal justice system and policing.

A flurry of technological reforms has characterised Chief Justice D Y Chandrachud of the Supreme Court's term. The Supreme Court asked all higher courts to ensure that no attorney is excluded from hearings held in hybrid facilities or by video conference. Previously, in the Article 370 case hearings, the CJI had asked solicitors to upload

1."Digital 2022: India," DataReportal – Global Digital Insights, 2022 available at: https://datareportal.com/reports/digital-2022-india (last visited March 26, 2024).

***Assistant Professor, The Central Law College, Salem, Tamil Nadu.**

their arguments and supporting documents to the internet.[2]

Legal research, predictive analytics, and case management can all be enhanced by the Indian judiciary's adoption of technology. To computerize court procedures and create a networked infrastructure, the E-court project, which was part of the National e-Governance Plan, was the catalyst for the modernization push. Information on cases that are pending or have been resolved is currently available in real time on the National Judicial Data Grid.[3]

However, how far can AI be applied in our current justice system? Can it make decisions for judges in place of people? This raises some concerns. Because there are two sides to the use of AI in the court, stakeholders must proceed cautiously.

While AI can be useful in courtrooms, it's important to consider the possibility that biased metadata or inaccurate information could lead to decision-making biases. Technology is necessary for the justice system to operate autonomously. However, it's crucial to keep in mind that people are behind those statistics. Artificial intelligence can become a useful ally as the Indian judiciary handles an increasing number of cases and demands for increased transparency.

Application of AI in Indian Judiciary

AI in Legal Research

Legal research is an inevitable tool that is used to systematically analyse a legal question concerning statutes, and precedents and give a solution to a legal question. This systematic analysis in law practice has to start with identifying the legal issue, searching related provisions of law, finding out the related case laws that are up to date, and interpreting them in a way to defend your client. This process of legal research helps the advocates to get deep down into the legal issue and understand it from its root cause which stays as a backbone for a case. It also makes them stay up to date regarding any issue. Legal research is not only used by advocates but also by researchers, para-legal workers, and students for their professional and personal development.

---

2. Hasan Mohammed Jinnah, "AI-powered courts can rewrite future of judiciary" The New Indian Express, 2023available at: https://www.newindianexpress.com/opinions/2023/Nov/02/ai-powered-courts-can-rewrite-future-of-judiciary-2629474.html (last visited March 25, 2024).

3. Ibid.

Conventional legal research involves visiting the library, looking into specific law journals, using legal citations to find the judgments, cross-referring them manually, and relying on legal texts to interpret them. Even though this was the basic method for doing legal research, it had its own cons as it was very time-consuming as we had to go through a laborious amount of data to find out something relevant. Not all libraries were equipped with all books and journals thus the physical access to all relevant data was a question. Sometimes the data can be outdated or incomplete which hinders the research. As the usage of computers developed, we tried to feed all the information to the system and made our work paperless and less taxing with all information from a single system.

The recent developments of AI in all fields have paved the way for making legal research less taxing and increasing accessibility to n number of cases through various jurisdictions. AI-driven research tools use algorithms and data to sort out digital information as per our needs. The most beneficial usage for Artificial Intelligence in legal research is that it can handle and analyze large volumes of data, find out data patterns etc, and give the desired result very quickly.[4] There is also a high accuracy rate for the results of such data when compared to human error. AI applications can be custom-made to suit the needs of the researcher. It can even analyse the legal principles used in each case and connect the cases with the same principle.

Artificial Intelligence can be used in Legal Research were

- ❖ There is large data set where it would take a long time to analyse the data if done manually using human labour
- ❖ When we have time constraints or deadlines which need to be met
- ❖ When you need to identify a pattern. For example – you want to know how many judgments were delivered using one legal principle
- ❖ While identifying a pattern we will also be able to see the predictive analysis of each case

Looking at the current trend of the judiciary and the number of cases, inclusion of AI will be apt in the area of legal research. In few instances it has already come into functioning like the introduction of

4. Akash Takyar, "AI for legal research: A new era of efficiency and accuracy" LeewayHertz - Software Development Company, 2024available at: https://www.leewayhertz.com/ai-for-legal-research/ (last visited March 22, 2024).

SUPACE and SUVAS by the Supreme Court of India.[5]

IIT Kharagpur researchers have developed an AI-assisted technology that can read court orders and judgements. To detect legal infractions, machine learning is also used.[6] AI is currently being used for contract analysis and review by Indian company Cyril Amarchand Mangaldas in partnership with Canadian AI assistance Kira Systems.[7]

Automated Document Analysis

Analysing contracts, documents and judgements which run down for many pages can be made easy by using Artificial Intelligence tools. Specific tools like natural language processing and machine learning can read through vast amount of data to extract the relevant information, identify the legal principles involved, categorize the details in custom made formats within few seconds. This process can help the human expertise to work in more complex issues.[8] Lawyers can access and manage their case files more easily, stay on top of deadlines, and automate repetitive tasks when such technology is integrated with case management software.

Predictive Legal Analysis

AI systems analyze old case data to predict potential case outcomes. The number of cases that are pending and the shortage of judges to make decisions on those motions are two of the judiciary's largest issues. Consequently, courts may use predictive analytics to address these problems by presenting the parties to a dispute with the likely results and encouraging them to reach an out-of-court settlement.[9] Both the court and the parties will benefit from this as it will help them avoid the drawn-out and difficult trial processes.

Case Management

Using AI to speed up case management processes allows judges to better organise and prioritise their caseload. Workflow management can be more effectively enhanced by automated systems in terms of

5. "FIVE notable applications of legal AI in India," INDIAaiavailable at: https://indiaai.gov.in/article/five-notable-applications-of-legal-ai-in-india (last visited March 22, 2024).

6. Harshul Gupta, "Scope of Artificial Intelligence as a Judge in Judicial Sector"(Indian Journal of Law, Polity and Administration, 2022)

7. Parth Jain, "Artificial Intelligence for Sustainable and Effective Justice Delivery in India" (Rochester, NY, 2018).

8. Dr. Bhavana Sharm, "Impact of Artificial Intelligence on the Legal Industry: Advantages, Challenges and Ethical Implications" (BioGecko Journal of New Zealand, 2023)

9. Parth Jain, "Artificial Intelligence for Sustainable and Effective Justice Delivery in India" (Rochester, NY, 2018).

scheduling, tracking deadlines, and monitoring.[10]

Decision Support System

To assist judges in making decisions, artificial intelligence (AI) systems may be used as decision support tools by giving them access to pertinent data, prior rulings, and legal analyses.[11] The judge always has the last say in all cases, and it is imperative to emphasize that artificial intelligence (AI) is merely a supporting tool.

Can Ai Be A Judge?

If AI is left to make decisions and replace human judgment it shall be intertwined between data security, privacy, human rights, and ethics. Many countries throughout the world have tried to include AI in the judicial sector. A few examples are, where AI tools are used to decide bail applications. Whereas some countries like Estonia have heavily implemented the use of Machine Language and Artificial Intelligence.12 As the Indian Judiciary is more conservative, allowing AI applications to decide is far away in accepted.

But if used it will help in shortening the time needed for decision-making by accelerating different phases of a case. Judges could be able to conduct trials more quickly and effectively as a result, which would shorten the time it takes to resolve cases. The problems of "dissimilar judgments in parallel cases" and "inconsistent use of law" can be ascertained as much as possible, which is beneficial for the harmonization of regional judicial norms.13 A standard judicial decision that "related cases are decided correspondingly" should be made because similar or parallel cases can have alike or like outcomes when the law is applied equally and consistently.14

Indeed, criteria based on identical case components, consistent modelling work, and standardised parallel processing operations could be extracted by artificial intelligence, assisting in ensuring case and

10. Cary Coglianese and Lavi Ben Dor, "AI in Adjudication and Administration" Brooklyn Law Review (2021).

11. Monika Zalnieriute and Felicity Bell, "Technology and the Judicial Role" (Rochester, NY, 2020).

12. "From Estonian AI judges to robot mediators in Canada, U.K. | LexisNexis Canada,"available at:https://www.lexisnexis.ca/en-ca/ihc/2019-06/from-estonian-ai-judges-to-robot-mediators-in-canada-uk.page (last visited March 26, 2024).

13. Krishna Ravishankar & Parul Anand, "AI Judges: The Question of AI's Role in Indian Judicial Decision-Making" CCAL, 2023available at: https://www.calj.in/post/ai-judges-the-question-of-ai-s-role-in-indian-judicial-decision-making (last visited March 22, 2024).

14. Ibid.

judge consistency with a comparable or equivalent algorithmic outcome for identical or similar cases. A trial knowledge atlas can quickly analyse the event and give judges positive feedback.

Inclusion of AI has its own challenges. Like how a nuclear fission can either be an invention or light up the cities and end up in destruction, AI also has two distinct sides. The biggest challenge in making AI judges is the usage of big data. Enormous amount of data feeding into the system is a big hinderance of proper administration. Even if the data is put into the system, the lack of structure for data is the primary challenge. Despite the fact that the cases have a general structure and involve similar time periods, judges present the facts in an individualistic manner. Even greater harm will result from similar cases that are not settled in a way that is consistent with judicial authority and social recognition. In such a situation we cannot overlook the degree to which society accepts the error rate of judicial artificial intelligence. Judiciary AI algorithms will unavoidably lead to bias and diverge from the neutral and objective path.

AI and Fundamental Rights

The core values of constitutional democracy as enshrined under Articles 14 and 21 can be listed as follows:

- ❖ Equal treatment
- ❖ Fairness
- ❖ Transparency and
- ❖ Due process

The right of all parties involved to be treated fairly, including an unbiased judge, a fair prosecutor, and a fair trial wherein any bias or prejudice for or against the accused is eliminated, was upheld by the Supreme Court in the case of Zahira Habibullah Sheikh and ors. v. State of Gujarat and Ors[15].It is therefore appropriate to assess the application of AI-enabled technologies through the prism of these values.

Inclusion of AI can indirectly include bias in their system. For example, when a judge is hearing a case and the predictive analysis tool tells the judge that the accused is a recidivist. In such a case, the judge blindly or without using his rational mind may increase the punishment as he is a recidivist. Due to technological anchoring, this biassed output can proceed unchecked and, in certain cases, even be encouraged, making judicial protection against bias inadequate. This inherent bias

15. AIR 2006 SUPREME COURT 1367

affects the quality of judgements rendered by the judiciary. As these AI systems need large volumes of data to process information another challenge which comes this way is that the end user does not know if relevant past information pertinent to the case has been used to make the decision. As the algorithm is opaque in nature it forms a black box phenomenon surrounding the decisions. Using these technologies without regards to any safeguards to the citizens increases the risk of discrimination against minority groups.

The judicial institutionalisation of racial bias was demonstrated by the COMPAS[16] system, an AI-based predictive model used for sentencing that was approved by the Wisconsin State Supreme Court in State v. Loomis.[17] The Fifth and Fourteenth Amendments of the United States Constitution's equal protection clauses are clearly violated by the racial bias. Similar concerns about the prejudice against Australia's indigenous tribes were voiced by the Supreme Court of Western Australia in the case of Director of Public Prosecutions for Western Australia v. Mangolamara.[18]

In the Indian context provisions against bias can be associated in Articles 14, 15, 16, and 17 read together. The courts have also ensured that judicial bias is against the concept of fairness in Shyam Singh v. State of Rajasthan.[19]

Acceptance by Judges

With the introduction of artificial intelligence (AI), judges may find it difficult to accept the evidence that is put before them. Addressing at the ASSOCHAM-organized 3rd IP Excellence Awards and Global IP Conclave, "Envisioning India's IP - Innovation Ecosystem for Viksit Bharat," Justice Dayal said,

> *"With the advent of AI, we are standing at the threshold of a very interesting, complex and difficult time where we may not be able to believe the evidence which is presented before us."*[20]

16. Natalia Mesa, "Can the criminal justice system's artificial intelligence ever be truly fair?" Massive Science, 2021available at: https://massivesci.com/articles/machine-learning-compas-racism-policing-fairness/ (last visited March 26, 2024).

17. "State v. Loomis" Harvard Law Review, 2017available at: https://harvardlawreview.org/print/vol-130/state-v-loomis/ (last visited March 24, 2024).

18. "McGlade, Hannah; Hovane, Vickie --- 'The Mangolamara Case: Improving Aboriginal Community Safety and Healing' [2007] IndigLawB 29; (2007) 6(27) Indigenous Law Bulletin 18,"available at: https://classic.austlii.edu.au/au/journals/IndigLawB/2007/29.html (last visited March 28, 2024).

19. 1973CRILJ441, 1972()WLN165

20. "Courts Facing 'Complex, Difficult' Time Due To AI: Delhi High Court Judge," NDTV.

It is still unclear as to how many judges will be ready to use AI applications in their day-to-day work. Judges using these technologies may be limited to the younger generation. Some senior judges may believe that the usage of AI may be unwarranted in justice delivery. Some may also have a notion not to give these machines control over the litigation process. They may also feel instead of using AI, they would much rather spend a significant amount of time deciding cases and delivering judgment.

Conclusion

Artificial Intelligence can be very helpful in many aspects in the legal filed as discussed above like legal research, document analysis and predictive policy. But if it is given the job of deciding cases, artificial Intelligence, and its related aspects of machine learning etc are very opaque in its functioning which has serious implications. This phenomenon may be called the black box phenomenon where the original decision-making process is not transparent to the end users. Non-availability of such crucial information is a concern that needs to be addressed. This can also be termed as the Black Box phenomenon.[21]

The Indian Judiciary has been a cornerstone in recognizing the fundamental principles of due process, transparency, and fairness in many cases like Maneka Gandhi Vs UOI[22] and Shiv Kumar Vs Hukam Chand[23]. India also has a firm precedent in recognizing that in natural justice every party must be given an equal opportunity to adduce the relevant information on which he relies to the judiciary. Therefore, the use of AI in deciding cases may blur out these recognized rights.

The inclusion of AI in the Indian Judiciary is still in the nascent stage and its usage in this domain will assist judges and advocates who are the pillars of judiciary. No matter how much technology grows or becomes advanced it can never replace a human judge. However, it can be useful in assisting them in dealing with large volumes of data which ultimately leads to the early completion of the proceedings. As it is widely accepted that "Justice Delayed in Justice Denied" Artificial Intelligence acts as a catalyst in enhancing the speed of justice delivery and guaranteeing the public long-lasting justice being accomplished.

comavailable at: https://www.ndtv.com/india-news/courts-facing-complex-difficult-time-due-to-ai-delhi-high-court-judge-5006419 (last visited March 28, 2024).

21. Krishna Ravishankar & Parul Anand, "AI Judges: The Question of AI's Role in Indian Judicial Decision-Making" CCAL, 2023available at: https://www.calj.in/post/ai-judges-the-question-of-ai-s-role-in-indian-judicial-decision-making (last visited March 28, 2024).

22. 1978 AIR 597, 1978 SCR (2) 621

23. AIRONLINE 2018 SC 866