

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

VOLUME 2 AND ISSUE 1 OF 2024

INSTITUTE OF LEGAL EDUCATION

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

APIS – 3920 – 0013 | ISSN - 2583-7990

(OPEN ACCESS JOURNAL)

Journal's Home Page – https://ijclp.iledu.in/

Journal's Editorial Page - https://ijclp.iledu.in/editorial-board/

Volume 2 and Issue 1 (Access Full Issue on - https://ijclp.iledu.in/category/volume-2-and-issue-1-of-2024/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in



© Institute of Legal Education

Copyright Disclaimer: All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer https://ijclp.iledu.in/terms-and-condition/

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY

VOLUME 2 AND ISSUE I OF 2024

APIS – 3920-0012 | ISSN - 2583-7990

Published by

Institute of Legal Education

https://iledu.in

"LEGAL ACCOUNTABILITY IN THE AGE OF AI: IDENTIFYING EMERGING RISKS"

AUTHOR - S. JAYASHREE, ADVOCATE, MADRAS HIGH COURT AS INDEPENDENT AUTHOR

BEST CITATION - S. JAYASHREE, "LEGAL ACCOUNTABILITY IN THE AGE OF AI: IDENTIFYING EMERGING RISKS", *INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY,* 2 (1) OF 2024, PG. 12-30, APIS – 3920-0012 | ISSN - 2583-7990.

ABSTRACT:

Due to technological development, Artificial Intelligence is everywhere. From the Healthcare sector to commerce, AI is influencing and indulging with the mankind in a day-to-day basis. But we are enjoying the benefits, without addressing the potential risks of AI. Recently the Star Life Insurance data theft shook the 31 million of its customers. It's not just about its customers, it's about the data privacy of 1.425 billion people in India. Data protection is not the only risks of AI, it can cause more, but what it could be done with upcoming Digital Personal Data Protection Act,2023 (yet to be implemented). Developing Country like India is struggling to introduce and implement the data protection legislation for the past two decade, on the other hand the European Parliament passed the Artificial Intelligence Act in March 2024. It shows India needs to work on robust legislations to protect the people digital rights. It has to be mentioned that the Zomato CEO, recently tweeted that he banned all its subscribed hotels and restaurants to use AI generative images of food which can mislead the images of real food. But whose responsibility is to protect citizens rights? and what are the legal accountability if AI is used to commit a crime? Hence, this research is to find out the emerging risks of AI and its implications. This study also attempts to suggest the possible remedies by comparing the international legislations.

Key words: Artificial Intelligence- Data privacy- EU-AI Act, 2024- DPDP Act, 2023– Accountability

INTRODUCTION:

The exponential rise of attributed electronic devices, systems, and networks has made cybersecurity far more challenging. This is worsened by developments in the digital economy and infrastructure, which have resulted in a considerable increase in cybercrimes with dangerous implications. Furthermore, studies note the ongoing development of nation-state-affiliated and criminal adversaries, as well as the rising complexity of cybercrimes, which are discovering new and intrusive methods to target even the savviest of targets.

Remembering Elon Musk quote about Artificial Intelligence, **"Mark my words, AI is more dangerous than Nuke"**. The vulnerable of crimes committed by AI is getting widened day by day. From the lay man to the national security is under threats in the hands of malwares. The number of Digital fraud cases were increasing rapidly. Deception and Phishing is can be the best example of how hackers can abuse AI techniques to develop a 'social bot', which can help them deceive and manipulate a person into complying with their request. These 'social bots' are algorithms designed to emulate human behaviour by producing content and interacting with users on the internet[1]. The sad part is even the well -educated persons fall for the trap and losing their hard -earned money. Spyware like Pegasus were used to track targeted victims, which caused storm waves in the Indian territory.

Check Point's Global Threat Index for September 2024 revealed its Global Threat Index for

[1] C. Freitas, F. Benevenuto, S. Ghosh and A. Veloso, "Reverse engineering socialbot infiltration strategies in Twitter", *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining*, pp. 25-32, Aug. 2015

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 2 AND ISSUE I OF 2024
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

September 2024. The report highlights an interesting trend in the cybersecurity landscape, particularly the emergence of artificial intelligence (AI)-driven malware, alongside the ongoing dominance of ransomware threats[2]. Researchers determined that the hackers likely utilized AI to create a script that delivered AsyncRAT malware via HTML sneaking. This approach includes transmitting a password-protected ZIP file containing malicious VBScript code to start a virus chain on the victim's device. The organized and documented code indicated AI assistance in its production[3].

However, most of the cybercrimes is committed by anonymity, uncertainty of the liability or legal accountability in the law, made the hackers misuse the AI applications without any hassle. In India, even after passing the Digital Personal Data Protection Act, 2023 in the Parliament, it's not implemented. "Delay in notification of rules has made the Act redundant" said by Aruna Sharama, former secretary, Ministry of Electronics and Information Technology (MeitY). This is the high time for the people in the rule to re-think whether India is ready to tackle the AI based risks.

The purpose of this article to examine the emerging risks of AI and focus on the ambiguity of legal accountability to those crimes. By comparing new EU-AI Act 2024, case studies, legal frameworks and other existing initiatives, it seeks to shed light on the urgent need for robust legislations. It is essential to achieve cyber security in the age of Artificial Intelligence.

RESEARCH QUESTIONS:

1. What are the emerging risks of Artificial Intelligence?
2. How can legal systems establish clear standards for determining liability when AI systems cause harm, especially in cases of autonomous decision making?
3. What regulatory frameworks are necessary to ensure the safe and ethical development of AI technologies, and how can these frameworks be implemented globally?
4. How have International legal frameworks and policies effectively addressed the issues when crimes committed by AI?
5. What are the socio-economic impacts of an algorithm - based crimes in the human society?

OBJECTIVES OF THE STUDY:

Identifying the emerging risks of Artificial Intelligence, especially focusing on legal accountability or liability issue is the main goal of this article. By looking at this subject, the study hopes to emphasise the importance of enacting a robust law and policies and enumerate the possible measurements to prevent the abuse of AI.

- Identify the risk factors of AI involved in the cyber sphere,
- Determine the standard of legal frameworks to deal with the algorithm - based crimes,
- To ascertain the ideal laws to protects people rights by comparing global laws,
- Determine the impacts and assessing the future generations towards ethical principles.

DEFINITION OF KEY CONCEPTS:

- **AI Systems**: Machine-based systems that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, contents, recommendations or decisions that can influence physical or virtual environments[4].
- **Cyber security:** the practice of protecting systems, networks, and programs from digital attacks

[2] By Check Point Team, Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks, Check Point Blog (July 16, 2024).
[3] Times of India's blog about Ai-powered-malware-emerges-as-new-threat-in-cybersecurity-landscape Available at: https://www.msn.com/en-in/money/news/ (Accessed: 21 October 2024).
[4] Article 3 of the European Union Artificial Intelligence Act 2024

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 2 AND ISSUE I OF 2024
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

- **Ethical principles of AI:** Accountability, Transparency, against to Bias and Discrimination, Privacy, Compliance and Reliability. These six principles are considered as Ethical Principles of AI.

HYPOTHESIS:

Uncertain legal accountability in AI can lead to a range of negative consequences, including increased risk of harm to personal information, erosion of public digital rights, regulatory challenges, and difficulties in achieving the global governance. To mitigate these risks, it is essential to develop clear and effective legal frameworks that address the unique challenges posed by Artificial Intelligence.

METHODOLOGY:

This research aligns with the principles of legal realism and interdisciplinary research. In according with the nature of the research work, the issues contained with this research topic and understanding and ease of reading, the researcher conducts this research based on combinations of doctrinal and empirical methods thereby conducting depth-study of the subject after exploring primary sources of questionaries responses collected from 50 samples to find out the legal awareness about recent data theft cases among degree holders and on doctrinal method, the secondary sources such as statutes, enactments, legislations, case laws, bills, national and international acts, policies, rules, regulations, law books, journals, articles and newspapers, etc were explored.

EMERGING RISKS OF AI:

The rapid evolution of artificial intelligence (AI) technologies is reshaping various facets of society, bringing both remarkable opportunities and significant challenges. As AI becomes more embedded in our daily lives, it is crucial to examine the emerging risks associated with its widespread adoption.

1. DEEPFAKES

Deepfake technology uses AI algorithms like generative adversarial networks (GANs) to produce synthetic material, including photos, videos, and sounds. Recently one of the songs in the Tamil film called G.O.A.T, features AI-generated voice of late singer Bavatharini[5]. Even in Hollywood film called Fast and Furious, used AI to make a particular scene by using images of late actor Paul walker. But the issues arises when AI used to create realistic misleading information that resembles actual people while making alterations.

Deepfakes was coined in 2018 by a Reddit user who started a community dedicated to developing and using deep learning algorithms to synthetically face swap female celebrities into pornographic films. According to a survey by Deep trace, an Amsterdam-based cybersecurity firm, deepfake pornographic movies are mostly aimed at women, worsening gender disparity[6]. Women make up 90% of the victims of crimes such as revenge porn, nonconsensual porn, and other types of harassment, with deepfake headlining the list. Celebrities are the main prey to hackers. Actors like Amitab Bachan, Anil Kapoor, Rashmika Mandana and Kajol are not exceptional to this abuse of AI. Some quoted as personal revenge and some instances quoted as entertainment as there is no explicit law to prohibit or regulate such AI's.

Anil Kapoor v. Simply Life India and Ors.

The Delhi High Court has extended protection to actors, individual personas, and personal qualities against exploitation, especially through AI technologies for making deepfakes. The Court ordered an ex-parte injunction that effectively prohibited sixteen (16) businesses from using the actor's name, likeness, image, and technical tools such as AI for financial benefit or commercial purpose[7].

[5] GOAT 2nd single: Vijay's track features late Bhavatharini's AI-generated voice - India Today (Jun 21, 2024 21:00 IST)
[6] Deep Trace, The State of Deepfakes, Landscape, Threats, and Impact https://regmedia.co.uk/2019/10/08/deepfake_report.pdf
[7] 2023 LiveLaw (Del) 857

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 2 AND ISSUE I OF 2024
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

Amitabh Bachchan v. Rajat Negi and Ors.

It was given an ad interim in rem injunction against the improper commercial exploitation of his personality rights and personal traits, including voice, name, picture, and likeness for commercial purposes[8].

Chaitanya Rohilla v. Union of India

Petition under article 226 of the constitution of India for the issuance of a writ of Mandamus inter alia directing the Respondent to lay down guidelines in Exercise of its powers under section 79 (2) (c) Read with section 87 (2) (zg) of the information Technology act, 2000. The Delhi High Court requested the government's answer on regulating AI and deepfake technology to avoid potential consequences including privacy infringement and economic loss[9].

Unlike celebrities deepfake, Political Persons deepfakes was mostly used to mass social manipulation, in March 2022, a video message from Ukrainian President Volodymyr Zelensky leaked on social media channels, in which the President was seen asking Ukrainians to lay down their guns and submit. As a result, the President's administration promptly disavowed the video's validity and labelled it as a profound fake. The film was the first high-profile use of deepfake during an armed war, marking a significant turning point for diplomatic warfare.

According to the "State of Deepfakes" report by Home Security Legends, online deepfake videos have surged by 550%, reaching nearly 95,820 instances in 2023, with India identified as the sixth most vulnerable country to this emerging threat[10]. In 2020, manipulated videos of Bharatiya Janata Party (BJP) leader Manoj Tiwari and Madhya Pradesh Congress chief Kamal Nath sparked controversy and highlighted the potential misuse of deepfake technology in political campaigns in India[11].

Deepfakes are not restricted to the generation of visuals and videos; as previously stated, AI techniques may be used to clone people's voices in order to carry out financial frauds. Approximately 47% of Indian people have encountered or know of someone who has undergone an AI voice fraud. According to McAfee's research on AI Voice Scams, over 83% of Indian victims reported financial losses, with 48% losing more than INR 50,000[12].

NATIONAL AND INTERNATIONAL LAWS GOVERNING DEEPFAKE:

A. INDIA:

In reaction to a viral deepfake video starring popular performer Rashmika Mandanna, the Indian government has issued a harsh warning to social media sites, emphasizing the legal rules controlling such deepfakes and the related penalties. This breakthrough has generated serious concerns regarding the use of artificial intelligence (AI) for deception.

The Ministry of Electronics and Information Technology has invoked Section 66D of the Information Technology Act of 2000, which deals with 'penalty for cheating by personation by exploiting a computer resource.' According to the clause, anybody found guilty of cheating through personation utilizing communication devices or computer resources faces a three-year jail sentence and a fine of up to one lakh rupees.

Other than aforementioned section, Rule 7 of the Information Technology Rules (Intermediary Guidelines and Digital Media Ethics) Code, 2021 (hereinafter referred to as the "IT Rules") would cause organizations to lose the protection provided by Section 79(1) of the IT Act[13]. Sections

[8] 2022 SCC OnLine Del 4110.
[9] W.P.(C) 15596/2023, CM APPL. 62399-62400/2023.
[10] Sarkar, Diya, and Sudipta De Sarkar. "Combatting Deep-fakes in India–An Analysis of the Evolving Legal Paradigm and Its Challenges." (2024).
[11] Bhaumik A, "Regulating Deepfakes and Generative AI in India | Explained" (The Hindu, December 4, 2023)
[12] https://www.livelaw.in/law-firms/law-firm-articles-/deepfakes-personal-data-artificial-intelligence-machine-learning-ministry-of-electronics-and-information-technology-information-technology-act-242916
[13] According to Section 79 (1) of the IT Act, online intermediaries are not liable for any third-party information, data, or communication connection that they make available or host. Rule 7 of the IT Rules allows aggrieved

67, 67A, and 67B of the IT Act explicitly prohibit and penalize publishing or sending obscene content, material involving sexually explicit acts, and minors shown in sexually explicit acts in electronic form, respectively. However, Digital Personal Data Protection Act, 2023 not explicitly govern deepfakes, but generally govern all the data fiduciaries for legitimate use of the data.

B. UNITED STATES OF AMERICA

Only a few of United States have approved legislation addressing new deepfake technology. Texas adopted S.B. 751[14], and California enacted AB730 in 2019[15]. Both of these rules prohibit the use of deepfakes, which might be used to influence future elections. In 2019, California's AB602, Georgia's S.B. 337, and Virginia's SB 1736[16] were all approved to prohibit the creation and dissemination of non-consensual deepfake pornography, while New York law S6829A introduced legal action against the unlawful publication of deepfakes in 2020.

In recent days, a number of legislations regulating artificial intelligence (AI) have been presented and adopted in many states until 2022. Although AI law has advanced in the US, most states have yet to initiate or adopt relevant legislation[17].

C. CHINA

China's government has established Deep Synthesis Provisions, which restrict the generation of deepfakes without user agreement and demand certification of AI-generated material. According to the new Chinese regulations, any content created using an AI system must be clearly labelled with a watermark, which is a text or image visually superimposed on the video indicating that the content was edited. The provisions apply to two types of entities: platform providers that provide content generation services and end-users who use such services. Content generation service providers must also promise not to process personal information. China's Cybersecurity Law and Detailed Implementation Rules for the Counter-espionage Law include prohibitions to prevent the publication or distribution of deepfakes sounds promising to the people in the country.

D. GERMANY

On July 5, 2024, the Federal Council of Germany (Bundesrat) presented a draft bill to the German Federal Parliament intended at criminalizing the protection of individual rights against deepfakes. The proposed law establishes a new criminal crime called breach of personality rights by digital forgery in the section 22 of the Bill. It makes it illegal to create and distribute media content that realistically reflects a person's look, conduct, or voice using computer technology without their agreement, punishable by up to two years in prison or a fine. The proposed legislation also contains safeguards for the deceased, enhanced penalties for aggravating circumstances, and exemptions for socially acceptable behaviour[18].

2. INVASION OF PRIVACY

The integration of AI into everyday life raises significant privacy concerns. AI systems often rely on vast amounts of personal data to function effectively, leading to questions about consent, data ownership, and surveillance. For example, smart devices collect continuous data from users, often without explicit consent. This data can be used to create detailed profiles, leading to targeted advertising and, in some cases, manipulation of consumer behaviour.

The Cambridge Analytica scandal, where personal data from millions of Facebook users was harvested without consent for political advertising, underscores the potential for misuse of personal information. To address these concerns, a comprehensive framework for data protection and privacy is necessary. This

persons to take platforms to court under the provisions of the Indian Penal Code.

[14] SB 751 (Texas), https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm.

[15] AB-730 (California), Aug. 13, 2019 version, https://leginfo.legislature.ca.gov/faces/bill.

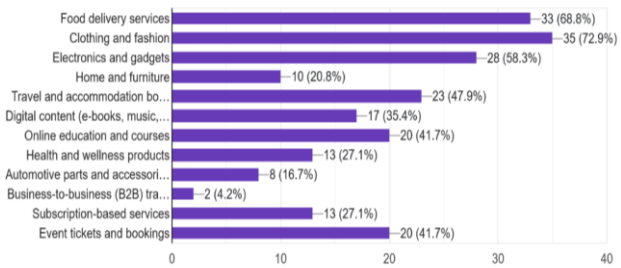
[16] HB 2678 (Virginia), http://lis.virginia.gov/cgi-bin/legp604.exe?191+ful+HB2678S1

[17] Jonathan Cedarbaum, Matthew F. Ferraro, and Brent Gurney, Bipartisan Group of Legislators Unveils Bill to Address Threat of "Deepfake" Videos, WilmerHale Client Alert, July 2, 2019

[18] Germany: Introduced Bill relating to criminal protection of personality rights against deepfakes - Digital Policy Alert

could involve stricter regulations on data collection practices, enhanced transparency requirements, and the establishment of user rights regarding data access and deletion. Even the educated persons failed to know the importance of data protection, over 136 crores of people living in this country but the awareness of the choice and consent is questionable. India, 3rd largest economic country, doesn't have the specific legislation to deal with data protection, through the Judicial activism, Supreme and High Courts protects the right to privacy of its citizen.

Recently the Irish Data Protection Commission fined LinkedIn €310 million for breaching GDPR by using personal data for targeted advertising without proper consent[19]. This case highlighted the importance of obtaining explicit consent for data processing. The Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield framework, ruling that it did not provide adequate protection for personal data transferred to the US2. It emphasizes the need for additional safeguards when transferring data to third countries. The Dutch Data Protection Authority, in cooperation with the French CNIL, fined Uber €290 million for transferring personal data outside the EU without sufficient guarantees[20].



This question was framed to find out what category of e-commerce that samples are using in prevalent and what are the other categories they opting for. Where out of 50 samples, 33 samples opting e commerce for food delivery services i.e 68.8%, 35 samples opting for clothing and fashion i.e 72.9%, 28 samples opting e commerce for electronic and gadgets i.e 58.3%, 10 samples for home and furniture i.e 20.8%, 23 samples opting for travel and accommodation bookings i.e 47.9%, 17 samples opting for digital content for e-books, music i.e 35.4%, 20 samples opted online education courses i.e 41.7%, 13 samples opted health and wellness products i.e 27.1%, 8 samples opted automative parts and accessories i.e 16.7%, business to business transaction was opted by 2 samples i.e 4.2%, subscription based services were opted by 13 samples i.e 27.1% and event based bookings was opted by 20 samples i.e 41.7%. hereby it is clear that clothing and fashion and food ordering was prevalent in India. During and After the COVID-19, the method of business, health, banking, food and cosmetic industries turned in electronic based, the transactions were replaced with digital payments method. The above questions demonstrate how often people are using data fiduciaries.

Not only European Data Commissioner, Even the French data protection authority, CNIL, fined Google €50 million for lack of transparency, inadequate information, and lack of valid consent regarding ads personalization[21]. This case involved cross-border data processing and highlighted the need for clear consent mechanisms. The UK Information Commissioner's Office (ICO) fined British Airways £20 million for a data breach that exposed the personal data of 400,000 customers[22]. This case involved cooperation between multiple EU data protection authorities to address the breach. The Luxembourg National Commission for Data Protection fined Amazon €746 million for processing personal data in violation of GDPR. This case involved multiple EU countries and showcased the complexities of cross-border data protection enforcement[23].

[19] LinkedIn has been fined over $300 million for violating European privacy rules. - The Verge
[20] Dutch SA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US | European Data Protection Board (europa.eu)
[21] The CNIL's restricted committee imposes a financial penalty of 50 million euros against GOOGLE LLC | European Data Protection Board (europa.eu)
[22] British Airways fined £20m for data breach affecting more than 400,000 customers | The Independent
[23] Amazon hit with $886m fine for alleged data law breach (bbc.com)

Human Rights Council resolution 48/4, discusses recent trends and challenges concerning the right to privacy. The report focuses, in particular, on: (a) the abuse of intrusive hacking tools; (b) the key role of encryption in ensuring the enjoyment of the right to privacy and other rights; and (c) wide-spread monitoring of public spaces. It highlights the risk of creating systems of pervasive surveillance and control that may undermine the development of vibrant and rights respecting societies[24], this report may bring possible solutions to the World right now to combat the risks around AI.

3. ALGORITHMIC BIAS AND DISCRIMINATION

One of the most pressing issues related to AI is the perpetuation of societal biases. AI systems, often trained on historical data, can reflect and amplify the biases inherent in that data. For instance, facial recognition technologies have been shown to misidentify individuals from certain racial and ethnic backgrounds at higher rates than others. A study by the MIT Media Lab revealed that commercial facial recognition systems had an error rate of over 30% for darker-skinned women, compared to less than 1% for lighter-skinned men[25]. This disparity raises serious ethical concerns regarding the deployment of such technologies in law enforcement and public safety. At present scenario algorithm-based systems were prevalent in Banks, Selection or rejection on Job applications, most importantly in healthcare services even in courts. Hence, it's necessary to regularise and govern the such kind of algorithms to avoid bias and discrimination.

COMPAS, or 'Correctional Offender Management Profiling for Alternative Sanctions', is a well-known example of an algorithmic system having discriminatory impacts[26]. COMPAS is utilized in some regions of the United States to forecast if a defendant will commit another crime. COMPAS is intended to assist courts in determining whether a person should be placed on probation (supervised release from jail). COMPAS does not consider ethnic origin or skin color as inputs. However, Angwin et al. found in 2016 that COMPAS is 'biased against coloured person'[27].

To mitigate these risks, it is essential to implement robust auditing processes for AI algorithms. This involves regularly reviewing and updating datasets to ensure they are representative and free from biases. Moreover, involving diverse teams in the development of AI systems can help identify potential biases before deployment. Creating guidelines for ethical AI development, which emphasize fairness and accountability, is crucial to fostering trust in these technologies.

For a variety of reasons, algorithms are frequently referred to be 'black boxes'. For example, most people lack the technical knowledge to grasp how such systems make judgments. Even specialists who have created an algorithmic system may not understand how it would behave when utilized in practice and given specific data. Additionally, commercial or state secrets may make it difficult to gain knowledge regarding algorithmic systems. People find it difficult to determine whether they were discriminated against since automated conclusions are not transparent. Another issue with non-discrimination legislation is that the prohibition on indirect discrimination lacks a clear black-and-white norm. The principle of indirect discrimination yields relatively broad norms, which are frequently difficult to implement in reality.

While indirect discrimination is vital in combating various kinds of algorithmic discrimination, the current assumption against direct discrimination is erroneous[28]. The effect of

[24] A/HRC/51/17: The right to privacy in the digital age | OHCHR
[25] Study finds gender and skin-type bias in commercial artificial-intelligence systems | MIT News | Massachusetts Institute of Technology
[26] See Equivant, 'COMPAS Classification', 2018, http://www.equivant.com/solutions/inmate-classification (accessed January 19, 2020).
[27] J. Angwin et al., 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks', *ProPublica*, May 23, 2016, https://www.ProPublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (accessed January 19, 2020).
[28] For further details, see C. Tobler, *Indirect Discrimination: a case study into the development of the legal concept of indirect discrimination under EC law* (Oxford:

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 2 AND ISSUE I OF 2024
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

US literature is somewhat predictable, given how closely the two paradigms have been linked throughout history. **Griggs v Duke Power Co, the foundational SCOTUS**[29] ruling on disparate impact, was a key factor in the CJEU's decision in **Jenkins v Kingsgate**[30], a conceptual cornerstone in the establishment of indirect discrimination. Today, however, US and European discrimination legislation cannot be ignored as readily as previously thought: the scope of direct discrimination is substantially broader than that of differential treatment.

Xenidis emphasizes the failure of EU discrimination law to address discrimination in a data-driven world, from intersectionality to arising novel blades of disparities. He also suggests that direct discrimination cannot capture cases where less favourable treatment is caused by correlations between an ADMS' (Algorithmic decision-making systems) features and protected characteristics. Echoing Hacker, she concludes that it would be 'challenging for algorithmic proxy discrimination to be regarded as direct discrimination'; instead, 'algorithmic proxy discrimination could be captured through the doctrine of indirect discrimination', despite the negative aspects of the resulting 'larger pool of justifications[31]'

A closer look at the mechanics of self-justifying feedback loops reveals a significant additional objection: if an algorithm recycles biased input to produce biased outcomes, the algorithm's 'predictive accuracy' may be completely incapable of sustaining a justification. Its forecast accuracy is only great because the world is skewed in predictable ways. **Enderby v Frenchay Health Authority**[32] (Enderby) provides a foundation for this reasoning, since an employer paid its majority female speech therapists less than its mostly male pharmacists. The health authority attempted to defend this divergence by claiming that the two professional groups had distinct collective bargaining processes that resulted in different conclusions. However, the Court of Justice rejected this plea[33].

Under the GDPR and the Data Protection Convention 108, businesses must complete a data protection impact assessment (DPIA) in specific circumstances. A DPIA is a procedure that systematically analyzes, identifies, and reduces the data protection risks of a project or plan[34]. Scholars including Goodman, Hacker, Kaminski, and Malgieri emphasize the potential of DPIAs to protect people from algorithmic prejudice[35].

The State Council of the People's Republic of China has proclaimed its goal to include artificial intelligence into the Chinese criminal justice system, involving the imposition of criminal punishments. This plan, nevertheless, has raised a number of troubling questions and concerns, including AI's misinterpretation of court decisions, its inability to make value judgments, possible algorithm biases, the diversity of data used by AI, the "black box" nature of AI sentencing, the public's decreased acceptance of AI-supported sentencing systems, the uncertain quality of algorithms, and so on. The favorable impact of AI on the objective of "same case, same sentence" should not be overestimated, and an unrestricted use of AI is prohibited.

The increased participation of AI in essential decision-making has created new ethical quandaries. The most pressing of these problems is the issue of prejudice and equality.

Intersentia, 2005); D. Pannick, *Sex Discrimination Law* (Oxford: Clarendon Press, 1985).

[29] *Griggs* v *Duke Power Co* 401 US 424 (1971) (*Griggs*).

[30] Case 96/80 *Jenkins* v *Kingsgate (Clothing Productions) Ltd* ECLI:EU:C:1981:80.

[31] Xenidis, *ibid*, 747.

[32] C-127/92 *Enderby* v *Frenchay Health Authority* [1993] ECLI:EU:C:1993:859. *Enderby* was an equal pay case, but equal pay caselaw is highly significant in the context of indirect discrimination claims: see the similarities between Equality Act 2010, s 19 and s 69(1)(b) and (2). In equal pay cases, the employer must identify a 'material factor' for a pay differential; if there is evidence that the factor is in some way 'tainted' by indirect sex discrimination, then the objective justification scheme applies: see *Glasgow City Council and others* v *Marshall and others* [2000] UKHL 5, [2000] IRLR 272.

[33] *Enderby ibid* at [20]-[23].

[34] CO, 'What is a DPIA?', https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/ (accessed January 19, 2020).

[35] B.W. Goodman, 'A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection' (29th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona), http://www.mlandthelaw.org/papers/goodman1.pdf (accessed January 19, 2020);

AI systems frequently draw on previous data, which may have inherent biases, resulting in biased outcomes in areas such as hiring, lending, and the criminal justice system. Another significant difficulty is algorithmic transparency. AI algorithms, viewed as "black boxes," make decision-making opaque, raising concerns about accountability and the ability to correct errors.

Chinese policymakers should consequently use extreme caution when using AI into sentencing. AI should be used as a "assistant" rather than a decision-maker, offering facts to courts and assisting them with sentencing judgments. In any case, the judges should make the final decision. Furthermore, algorithms should be transparent so that judges may examine their operation. A Committee overseen by the Chinese Supreme Court should be formed to ensure the quality of judicial data used by AI and to run a centralized AI system for sentencing[36]. These methods would help to maximize the use of court data and to implement a fair, accurate, and efficient sentencing system.

In India, "Search bias, algorithmic bias, and biased AI models are serious breaches of the safety and trust duties imposed on platforms by rule 3(1)(b) of the Indian IT regulatory framework. Those who are aggrieved by this can file FIRs against such platforms, and the safe harbor/immunity under section 79 will not apply in these situations[37]." which was clarified by the IT Minister.

The safe harbour clause, found in Section 79 of India's Information Technology Act of 2000, grants internet and social media platforms legal immunity from information uploaded by platform users. Though the IT Act 2000 makes no particular rules for regulating AI, platforms like as Google Bard, which are considered as intermediaries, are nevertheless subject to the law. According to media sources, the impending Digital India Bill, which will replace the IT Act of 2000, is likely to include provisions for AI regulation as well as outline standards and principles for responsible AI use.

4. ADVERSARIAL SOCIO-ECONOMIC IMPACT

Countries around the world are becoming increasingly aware of the potential economic and social benefits of developing and applying AI. For example, China and U.K. estimate that 26% and 10% of their GDPs respectively in 2030 will be sourced from AI-related activities and businesses. There has been tremendous activity concerning AI policy positions and the development of an AI ecosystem in different countries over the last 18 to 24 months – the US published its AI report in December 2016; France published the AI strategy in January 2017 followed by a detailed policy document in March 2018; Japan released a document in March 2017; China published the AI strategy in July 2017; and U.K. released its industrial strategy in November 2017[38]. At the same time, we need to address the potential adversarial risk of AI, that can impact the economic and societal growth of the country.

AI's potential to disrupt the labour market is another critical area of concern. Automation driven by AI technologies threatens to displace workers in various industries, particularly those involving routine tasks. A report by McKinsey Global Institute predicts that up to 375 million workers may need to switch occupational categories due to automation by 2030[39]. This transition poses significant challenges, especially for those in low-skilled positions who may struggle to adapt to new roles.

To mitigate the economic impact of AI, it is essential to invest in education and retraining programs. Policymakers should prioritize initiatives that equip workers with the skills necessary to thrive in an AI-driven economy. This includes promoting STEM education and

[36] Artificial Intelligence, Algorithms and Sentencing in Chinese Criminal Justice: Problems and Solutions | Criminal Law Forum (springer.com)
[37] Platforms with algo biases not protected under IT rule: Chandrasekhar | India News - Business Standard (business-standard.com)
[38] National Strategy for Artificial Intelligence (niti.gov.in)
[39] 375mn jobs to be displaced by automation by 2030 – McKinsey | Technology Magazine

fostering partnerships between businesses and educational institutions to create relevant training programs. Additionally, implementing safety nets, such as universal basic income or job transition assistance, can help support those affected by job displacement.

Although AI can have a beneficial environmental influence, such as allowing smart grids to meet energy demand or creating smart and low-carbon cities. However, one of the downsides of artificial intelligence is that it might cause major environmental damage owing to its high energy consumption. A 2019 study discovered that a certain sort of AI (deep learning in natural language processing) has a significant carbon footprint due to the fuel required by the hardware. According to experts, training a single AI model emits 300,000 kg of CO2, which is about comparable to 125 round-trip flights from New York to Beijing or five times the lifetime emissions of the average (American) automobile. Furthermore, model training is not the only source of emissions. Big tech's AI adoption has a substantial carbon effect due to the requirement to build data centers and mine and transport minerals.

4.1 LEAD TO TECHNO SOLUTIONISM

Big Tech corporations dominate artificial intelligence. Since 2007, Google has acquired at least 30 AI businesses focusing on everything from image identification to more human-sounding computer voices, establishing a vast monopoly on AI technology. However, Google is not the only gatekeeper. In 2016, Google, Apple, Facebook, Microsoft, and Amazon, as well as the Chinese mega players, spent up to $30 billion on AI-related research, development, and acquisitions, out of a total worldwide budget of $39 billion. Companies taking up AI businesses internationally is problematic because they will have an excessive role in defining the path of AI technology. With dominant positions in search, social media, online shopping, and app stores, these businesses have near-monopolies on user data and are emerging as the key AI providers to the rest of the sector. Concentrating power in the hands of large digital giants poses a risk of dictating policies to democratically elected governments.

Even it impacted on children and students, they urged to find a quick solution with the help of AI, chat bots rather than using their brains and asking the concern teachers, parents and even not ready to check with reality, this caused reliability issue and distancing with the society. On the other hand, loneliness-depression is one of the main concerns of the world right now, it increasing day-by-day, but studies found that these chat box AI's are helping those to fight loneliness.

5. UNCERTAINITY IN LEGISLATIONS

The security of personal data transported across national boundaries has been a driving force behind worldwide agreement on the core principles of data protection. For example, the OECD Privacy Framework (OECD 2013) states that a data controller "remains accountable for personal data under its control without regard to the location of the data" (adopted in 1980 and revised in 2013, Article 17).

However, because of uncertainties about data privacy rules in other countries, several nations restrict extraterritorial transfer of personal data. Such transfers may be approved under specific conditions or where a third country's data protection regulations are judged appropriate. This is especially important when dealing with personal information for national ID, civil registration, and voter registration systems. Legal frameworks may require regional or worldwide interoperability or mutual recognition of ID systems, in addition to data movement across borders. The research also reveals that the majority of enterprises who worry about legal uncertainty see considerable differences between the different EU data economy legislation (such as the Data Act) and the GDPR.

"Legal certainty is a fundamental requirement for value generation in an innovative economy. As a result, the legal issues in the GDPR must be resolved as soon as possible before new restrictions are implemented. Otherwise, the problems will simply move," says Wernicke. "Now

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 2 AND ISSUE I OF 2024
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

is the appropriate moment for this. The GDPR specifies a quadrennial examination in the second quarter of 2024. Use this to ensure GDPR requirements are both practical and legally safe.

In India, after enacting the rules and guidelines only we can address if there is any uncertainty or ambiguity arise, otherwise the Information Technology only prevail. But it does not mean there is robust law in India. For an example the Right to be forgotten was exercised through the Supreme Court Judgement on **K.S Puttaswamy v. Union of India**[40], based on GDPR, but even the DPDP Act,2024 was not officially recognized the right.

Another notable issue was there is no specific law to regulate cross- border data flow for all over the world. Every country has their own rules for data protection. GDPR restriction upon cross- border data flow makes hard for the non-EU small -scale industries to do business in European Union. If any breaches occurred the Jurisdiction is another grey issue to resolve.

6. SOCIAL MANIPULATION DURING ELECTIONS

Using AI for social influence during elections has major ramifications. Deepfakes and misinformation can weaken public faith in the voting process. This manipulation may also create societal differences and polarize voters, making it more difficult to reach agreement and togetherness. Furthermore, AI may study and use personal data to influence voter decisions, possibly changing the outcome of elections. Furthermore, the use of AI for manipulation creates serious legal and ethical problems, such as breaches of privacy and the integrity of democratic processes. These effects underline the need for strong rules and ethical norms to guarantee that artificial intelligence is utilized responsibly in elections.

More recently, Argentina became a testing ground for AI, with presidential contenders using deepfakes to represent each other negatively. While Javier Milei was represented as a cuddly lion, his competitor, Sergio Massa, was portrayed as a Chinese communist commander. In April 2023, the Tamil Nadu government was faced with a deepfake issue when cabinet minister Palanivel Thiaga Rajan (PTR) stated that two leaked audios of him reportedly ranting against CM MK Stalin's family were fakes. PTR was forced to quit as finance minister, and in the cabinet reshuffle, he was assigned the charge of IT ministry[41].

According to a VICE article, the BJP IT Cell's collaboration with The Ideaz Factory, a political communications business, in 2020 to generate "positive campaigns" utilizing deepfakes marked its debut in Indian elections. With election season starting, multiple doctored films have appeared online, many of which are from the renowned game show Kaun Banega Crorepati (KBC). Political groups on both sides of the aisle have shared modified footage. But who will control this? Probably the electoral commission, as it is in control throughout the election period[42].

In January, a fake replication of US President Joe Biden's voice was used in robocalls designed to deter Democrats from voting in the New Hampshire presidential primary[43]. During this year's Slovakian parliamentary elections, a deepfake audio clip of a lawmaker discussing electoral cheating went viral online. Despite leading the polls, the candidate ultimately lost the race[44].

SINGAPORE POSITION:

Singapore's parliament enacted legislation prohibiting deepfakes and other digitally modified information from candidates during elections. The Elections (Integrity of Online Advertising) (Amendment) Bill, introduced by the Ministry of Digital Development and Information (MDDI) last month, prohibits the

[40] Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1

[41] Indian politician blames AI for alleged leaked audio - Rest of World
[42] https://www.boomlive.in/law/elections-pornography-laws-on-technology-deepfake-artificial-intelligence-23656
[43] Deepfake Audio of Biden Alarms Experts in Lead-Up to US Elections (yahoo.com)
[44] A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning | CNN Politics

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 2 AND ISSUE I OF 2024
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

publication of digitally generated or manipulated content during elections that accurately depicts a candidate saying or doing something they did not say or do.

Social media services that fail to comply may be fined up to $1 million upon conviction, while all others may be fined up to $1,000, jailed for up to a year, or both[45].The new measure will not cover AI-generated or animated characters and cartoons, cosmetic alterations such as the use of beauty filters, or colour and lighting adjustments of images and videos, and entertainment content like memes.

7. DATA SOURCING AND CYBER ATTACKS

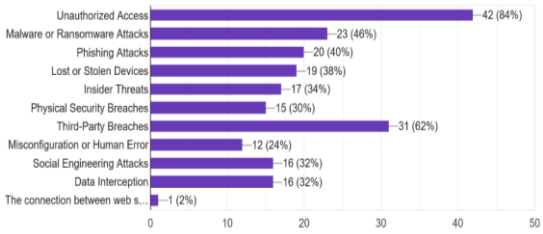
When compared to traditional software, generative AI has fewer barriers, making it easier to use, but it is also extremely adaptable. As a result, the development of generative AI will have a wide range of implications for cyber security. As of this writing, there have been no instances of wholly novel cyberattacks employing generative AI, although there is little question that some cyber attackers are already using it. We believe it is being utilized to increase the sophistication and efficiency of existing cyberattacks, as explained below.

Fraudulent use of email and false news production for phishing and business email compromise (BEC) objectives.

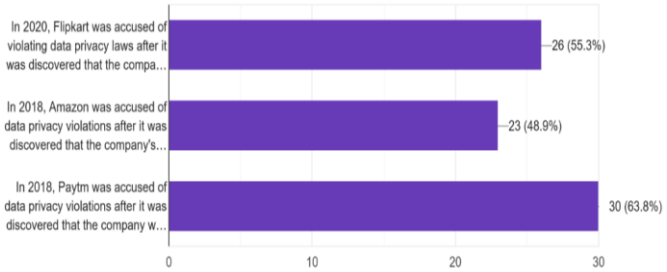
Malware creation assistance: sophisticated malware is difficult to construct with only the existing generative AI, but competent attackers utilize it as a programming help tool to boost creation efficiency.

Pre-attack investigation and reconnaissance support: automation and efficiency of human decision-making.

While the guardrails included into generative AI should have prevented these negative applications, attackers have perfected adversarial prompts to evade them. Generative AI developers have tightened the constraints, and there is now generative AI that is customized for cyberattacks with no output restrictions and marketed to cyber attackers as a black market. However, cyber attackers aren't the only ones that gain from generative AI. To counteract cyberattacks, CSIRTs and security operations centres (SOCs) will need to actively deploy generative AI. In the future, completely automated defensive systems might prevent fully automated cyberattacks.



It is necessary that people should know what constitute data breach, so this question was framed in their opinion what are all constitute data breach, where unauthorised access was opted by 42 samples which is 84%, malware or ransomware attacks opted by 23 samples i.e 46%, phishing attack opted by 20 samples i.e 40%, Lost or stolen devices data opted by 19 samples which is 38%, insider threats opted by 17 samples i.e 34% and physical security breaches opted by 15 samples, third party breached by 31 samples, misconfiguration or human error opted by 12 samples, social engineering attacks and data interception opted by 16 samples each and the connection between web was opted by 1 sample but actually the above said all options were example of data breaches.

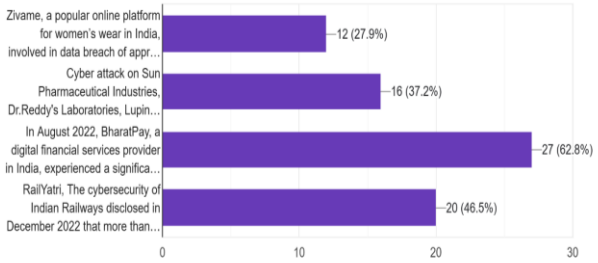


The following 2 questions were set of famous cases that shook the internet in past 3 years. To find out whether people are aware about these incidents these questions were framed. Flipkart

[45] Bill passed to counter digitally manipulated content, deepfakes during elections | The Straits Times

INTERNATIONAL JOURNAL ON CYBERSPACE LAW AND POLICY
VOLUME 2 AND ISSUE I OF 2024
APIS – 3920-0012 | ISSN - 2583-7990
Published by
Institute of Legal Education
https://iledu.in

data breach issue was known by 26 samples, amazon data breach issue was known by 23 people and paytm data breach issue was known by 30 samples.



Following by previous question, zivame data breach issue was known by only 12 samples, cyber-attack on famous pharmaceutical companies known by 16 samples and Bharatpay data breach issue was known by 27 samples and Railyatri data breach issue was known by 20 samples. Without knowing the data breach people are using these e-commerce platforms in prevalent is showing a pathetic condition of people about their concerns over data protection and the irresponsibility of the country without having regulatory mechanisms.

7.2 A LACK OF ETHICAL PRINCIPLE

The only reason for all the abuse and misuse of Artificial Intelligence is a lack of ethical principles. The OECD AI Principles are the first intergovernmental norm on artificial intelligence. They advocate for creative, trustworthy AI that upholds human rights and democratic ideals. They were adopted in 2019 and will be revised in 2024. They consist of five values-based principles and five suggestions that give practical and adaptable direction for policymakers and AI players[46]. That is,

- Inclusive growth, sustainable development and well-being
- Human rights and democratic values, including fairness and privacy
- Transparency and explainability
- Robustness, security and safety
- Accountability

8 SOCIAL SURVEILLANCE WITH AI TECHNOLOGY

Clearview Face Recognition Scandal is the best example social surveillance by AI can make adverse effect on society. Clearview is an artificial intelligence firm that developed a facial recognition technology to assist police officers in identifying criminals. They say that their software has assisted law enforcement in tracking down several paedophiles, terrorists, and sex traffickers.

However, in January 2020, The New York Times published a lengthy article detailing how Clearview made a mockery of data privacy by extracting about three billion photographs of users from social media sites such as Facebook, YouTube, Twitter, Instagram, and Venmo to construct the AI system[47]. Mr. Ton-That, the CEO, said that the algorithm solely harvested public photographs from these networks. Surprisingly, in an interview with CNN Business, the program retrieved the photographs from the show's producer's Instagram account. Google, Facebook, YouTube, and Twitter sent stop and desist letters to Clearview, preventing them from scraping photographs from their platforms. However, the photographs you shared online may be used in that AI program without your awareness. If a corrupt police officer uses this software or the system generates false positives, innocent individuals may be subjected to police investigations.

MASS SURVEILLANCE IN CHINA:

In recent times, China has faced harsh criticism for extensive monitoring of its citizens without

[46] AI principles | OECD

[47] Unmasking a Company That Wants to Unmask Us All - The New York Times (nytimes.com)

their agreement. They utilize over 200 million surveillance cameras and face recognition to keep a close eye on its citizens. China also harvests the behavioural data recorded by the cameras. To make matters worse, China created a social credit system that rates its residents' reliability and assigns grades based on monitoring. People with good credit scores receive additional benefits, while those with poor credit scores do not. The worst thing is that AI-based monitoring determines all of this without people's awareness or consent.

EU POSITION:

The "AI Act" restricts AI applications that pose significant dangers to basic rights, notably workplace monitoring. It firmly bans AI technologies that allow for indiscriminate or unjustifiable surveillance or monitoring of personnel. This policy attempts to limit employers' use of AI for surveillance purposes, protecting employees' privacy and dignity. This legislative framework enables responsible and ethical use of AI technology in the workplace, balancing technical progress and individual rights.

One of the most visible kinds of biometric mass surveillance is the use of live face recognition (or other biometric surveillance, such as recognition of people's eyes, ears, or gait) to track them around public locations. This can notify whomever is utilizing the system of the identify of everyone in a certain location in real time.

When deployed in London, for example, these systems consistently misidentified persons (particularly black men), and despite police claims of high success rates, were only approximately 19% accurate. People who attempted to avoid passing by these cameras or used their lawful right to oppose by hiding their faces were stopped and, in some circumstances, punished. The AI Act will, in theory, forbid police use of live public facial recognition and other biometric identification systems throughout the EU once it takes effect. This is known as "real-time remote biometric identification in publicly-accessible spaces for the purpose of law enforcement."

STATUS IN INDIA:

According to stories in The New Indian Express and Medianama, 800,000 lines of data, including the personal information of more than 50,000 people, were made public by a breach in the Tamil Nadu Police Facial Recognition Portal. A group identifying itself as "Valerie" was responsible for the hack, which was made public by threat intelligence platform FalconFeeds.io. Police officer identities, phone numbers, station information, and first information report (FIR) details are among the material that has been discovered for sale on the dark web after being taken from five different types of data sets. Authorities in India are still enthusiastically implementing facial recognition systems despite the possible danger of storing enormous honeypots of biometric data that are susceptible to breaches and assaults.

According to India Today, in an effort to discourage criminal activities, the government of Meghalaya, located in Northeast India, plans to install 300 facial recognition cameras and algorithmic software across Shillong. "Work is already underway, with high-level cameras being installed at various junctions," said Chief Minister Conrad Sangma. Police in Jammu and Kashmir have implemented an AI-based face recognition system to keep an eye on cars traveling through a tunnel on the Jammu-Srinagar National Highway, according to a report in News Intervention. High-focus CCTV cameras in the system record and compare the faces of drivers and passengers to a database of pictures of criminals, overground workers, and terrorists.

According to Medianama, in order to convert its current Automated Fingerprint Identification System (AFIS) to the Automated Multimodal Biometric Identification System (AMBIS), the Telangana State Police Department is looking for a service provider. The new Criminal Procedure (Identification) Act, 2022, which

grants law enforcement additional authority to gather biometric information including fingerprints, footprints, iris scans, and face photos, is what prompted the action.

The use of biometrics in India has been interwoven in the daily lives of the working environment, whether private or government. This digital transformation had driven the largest initiatives in India, such as Aadhaar and DigiYatra1 2. Both rely on distinct authentication methods to identify and authenticate persons. Research done by NITI Aayog as part of its National Strategy on Artificial Intelligence,3 on Digi Yatra (hereinafter referred to as the "Study") raised data privacy issues about the usage of facial recognition technology (hereinafter referred to as the "FRT") in India[48]. Digi Yatra employs Facial Recognition Technology to confirm passengers' travel credentials, enabling automated checks with minimum human participation at airports.

9 AUTONOMOUS WEAPONS

AI systems can currently use data autonomously, forecast human behaviour, collect intelligence, conduct surveillance, identify possible targets, and make tactical judgments in virtual battle. The employment of robots in the military is becoming more prevalent, and the transition to completely autonomous robots specialized for battle is now feasible. The fundamental question now is not what sorts of L.A.W.S could exist, but whether they constitute a significant risk to humans.

These "slaughterbots" aren't just fiction. In 2018, one of these drones nearly murdered Venezuela's president, and an experienced hobbyist could build one today for less than $1,000. All parts are accessible for purchase online, and all open-source technology may be downloaded. This is an unforeseen effect of AI and robots becoming more widely available and affordable. Imagine a $1,000 political assassin! And this is not a hypothetical threat for the future, but a real and present risk.

In the war between Russia and Ukraine, video footage shows drones going deep into Russian territory, more than 1,000 kilometres from the border, and destroying oil and gas infrastructure. Experts believe that artificial intelligence (AI) is helping to steer the drones to their targets. For such weapons, no one must hold the trigger or make the ultimate choice to detonate[49]. There are also insufficient worldwide rules covering the use of militaristic AI. While the United Nations and the European Parliament have proposed a prohibition on the use of deadly autonomous robots in warfare, issues remain regarding how the weapons might be controlled and if regulation would violate state sovereignty.

However, autonomous weapons have some advantages. Autonomous weapons can save troops' lives if conflicts are conducted with machines. Furthermore, in the hands of a responsible military, they can assist soldiers in targeting just combatants while avoiding accidentally killing friendly forces, children, and bystanders (similar to how an autonomous car can stop for the driver when a collision is near). Autonomous weapons can be employed to defend against assassins and offenders. However, the disadvantages and liabilities significantly exceed the benefits. The strongest such liability is moral—nearly all ethical and theological systems see the taking of a human life as a problematic act that necessitates extensive explanation and examination. The United Nations Secretary-General, António Guterres, has said **"The prospect of machines with the discretion and power to take human life is morally repugnant"**[50]

In 2015, the Future of Life Institute issued an open letter regarding AI weapons, saying that "a global arms race is virtually inevitable[51]." Such an escalating dynamic is familiar territory, whether in the Anglo-German naval weapons race or the Soviet-American nuclear arms race.

[48] Responsible for AI, Adopting the Framework, A Use case study approach on Facial Recognition Technology

[49] Lethal AI weapons are here: how can we control them? (nature.com)
[50] AI Weapons Are the Third Revolution in Warfare - The Atlantic
[51] Autonomous Weapons Open Letter: AI & Robotics Researchers - Future of Life Institute

Powerful countries have traditionally competed for military superiority. Autonomous weapons provide several opportunities to "win" (smallest, quickest, stealthiest, most deadly, and so on).

The International Committee of the Red Cross (ICRC) has suggested that nations implement new legally enforceable standards for autonomous weapons. New laws will serve to reduce major dangers to civilians and address ethical issues, while also providing legal clarity and stability.

- First, unexpected autonomous weapons should be outlawed. That is, autonomous weapons that are built or deployed in such a way that their consequences cannot be fully understood, predicted, or explained, including those that 'learn' targets while in use and maybe machine learning-controlled autonomous weapons in general.
- Second, autonomous weapons that are developed and used to direct force on humans should be forbidden.
- Third, strong limitations must be placed on the design and usage of all other autonomous weapons in order to reduce the hazards stated above, assure legal compliance, and address ethical issues.

It also suggests to enact a robust law to regulate or ban the AI weapon for various ethical reasons and more fully these rules could be set out in a new Protocol to the **Convention on Certain Conventional Weapons (CCW)**, or another legally binding instrument[52].

AI's LEGALITY IN INTELLECTUAL PROPERTY RIGHTS

The rapid advancement of AI technologies has raised critical questions regarding their impact on intellectual property within digital marketplaces. It is important to know how AI-driven innovations may inadvertently compromise copy rights in the e-commerce sector. Recently a group of Authors filed a case against 'Anthropic', an AI start up for committing large scale theft, alleging its popular chatbot Claude pirated the legally copyrighted books in its training. Last year The New York Times sued Google's OpenAI and Microsoft's Copilot for using its millions of copyrighted articles to train chatbots[53]. Without obtaining consent or copy right AI was being defended that it comes under the fair use doctrine as Informational to the society.

Whereas the AI based companies profited billions of dollars out of this infringement. The Report published by CVL Economics namely "Future Unscripted: The Impact of Generative Artificial Intelligence on Entertainment Industry Jobs" predicted 204000 entertainment industry jobs may be disrupted by GEN-AI over the next three years[54]. Because now GEN-AI were used to create literary artistic works. The worst part is, its significantly leads to questioning the authenticity of artistic work and largely concerning about whether there is any possibility of legal shift where companies can claim copyright over AI generated things? This ambiguity arises where Indian Copy right Act,1994 grant copy right for computer generated things. It's high time to consider the current situation where US Copy Right Office cancelled the given certificate of Graphic Novel "Zarya of the Dawn" but only to AI generated images not to the comics[55]. Hence, this research underscores the need for enhanced legal safeguards to protect the copy rights that can keep pace with this digital era.

The advancement of AI and related technologies raises concerns regarding the protection of innovation itself and the application of intellectual property rights (IPRs) to materials, content, or data produced by AI and related technologies, which can be artistic or industrial in nature and offer a variety of commercial opportunities; in this context, it is crucial to distinguish between creations that are autonomously generated by AI and those that are assisted by AI;

[52] What you need to know about autonomous weapons | ICRC

[53] New York Times Sues OpenAI and Microsoft: 'Billions' Owed for AI Copyright Infringement, Case Claims

[54] The Animation Guild: Future Unscripted: The Impact of Generative AI on Entertainment Industry Jobs - INDAC

[55] AI-generated comic artwork loses US Copyright protection - Ars Technica

Takes note of the European Data Strategy and the Commission White Paper on "Artificial Intelligence - A European approach to excellence and trust"[56]; emphasizes that the strategies described therein are likely to help unlock the potential of human-centered AI in the EU; however, it points out that the Commission has not addressed the issue of IPR protection in the context of the development of AI and related technologies, despite the critical importance of these rights; emphasizes the need for a single European data space and feels that its use will be crucial for innovation and creativity in the Union economy, which should be encouraged; emphasizes that the Union should be a key player in establishing fundamental guidelines for the creation, use, and usage of AI without obstructing its progress or preventing competition;

10 LIABILITY ISSUE IN CRIMINAL ACTIVITY

Liability in AI- based criminal activity is complex in nature. Who will be liable if the AI was misused, the developers and programmers or user or supervisory personnel or the organisation, or the people who are shared the same in social media or the same society that being regressive as victim blaming for centuries. Depending upon the nature of crime, mens rea, the damages, whether it for money or revenge or for proving superiority, what is the measure for the punishments if there are no certain laws is there to regulate. How complex is it? Right.

Hugh Nelson, a 27-year-old from Bolton, UK, has been sentenced to 18 years in jail for using artificial intelligence to produce pictures of child sexual assault[57]. He utilized Daz 3D, a 3D modelling tool, to turn harmless photographs of youngsters into pornographic stuff. This case was innovative because it utilized AI-generated graphics, which challenged conventional legal standards of obscene material. The inquiry needed coordination among numerous agencies, including Greater Manchester Police, the Crown Prosecution Service, and the National Crime Agency. Sunil Bharti Mittal, Chairman of Bharti Enterprises, had a personal experience with an AI-powered fraud in which a scammer utilized AI to clone his voice and demanded a significant sum of money from his executive in Dubai[58]. Mittal was startled when he heard the recording because the voice was so believable. This instance demonstrates the sophistication of AI technologies in perpetrating fraud, as well as the importance of remaining vigilant to avoid similar schemes.

India must combine technology expansion with strict regulatory constraints to promote innovation and prevent exploitation of AI. To successfully respond to AI-driven criminal risks, the legal system must strike a balance between promoting technological innovation and protecting individual rights. International collaboration and information exchange are vital for combating transnational cybercrime and AI-related illicit activities. AI's engagement in criminal activities in India raises several legal concerns that require a proactive and comprehensive solution from the legal community. As AI technology advances, it is critical to continually examine and adjust legal frameworks to address the ever-changing panorama of AI-related crimes[59]. Maintaining a balance between innovation and regulation is vital for harnessing the potential of AI and preventing its exploitation for illicit purposes. By tackling these difficulties and collaborating, India can create a strong legal framework that protects against AI-related crimes while promoting technology advancements for the betterment of humanity.

The notable issue in these types of criminal activities is finding the whereabouts of the criminals, most of the cyber crimes based on AI, can be done in anywhere from the world, then how a country can take necessary action

[56] REPORT on intellectual property rights for the development of artificial intelligence technologies | A9-0176/2020 | European Parliament
[57] AI Misuse Case: Man Sentenced to 18 Years for Child Sexual Abuse Images - TechStory
[58] Sunil Mittal exposes AI scam, says "my voice was perfectly articulated" in cloning attempt (msn.com)
[59] Artificial intelligence and criminal liability in India: exploring legal implications and challenges by Hifajatali Sayyed at https://www.tandfonline.com/doi/pdf/10.1080/23311886.2024.2343195

against the criminals[60]. In early 2022, Thai criminals utilized deepfakes to imitate police officials during extortion video conversations. This advanced application of AI technology made it impossible for victims to discern between genuine and false interactions, resulting in large financial losses. Cybercheck, an AI program utilized in thousands of criminal cases across the United States, has faced legal concerns over its accuracy and dependability. Défense attorneys have complained that the tool's methodology is obscure and hasn't been properly examined, raising worries about due process[61]. Recently in February 2024, a global company's Hong Kong branch lost US$25.6 million due to a deepfake video conference call impersonating its chief financial officer. This example highlights the potential of AI being exploited in complex financial frauds[62].

Creating thorough legal frameworks is critical for defining the roles and liabilities of AI developers, operators, and consumers. Implementing extensive audit trails can help to document AI activities and choices, facilitating accountability and investigations. Insurers that validate AI algorithms can shield policyholders from potential lawsuit expenses resulting from AI-related mistakes. Recognizing corporate criminal responsibility for AI providers guarantees that businesses are held accountable for misuse. Adapting the negligence regime to incorporate circumstances of "foreseeable foreseeability" makes deployers accountable for unanticipated AI behaviour. Finally, increasing international collaboration ensures that AI rules are uniform across countries. These solutions strike a balance between innovation and responsibility, ensuring AI technologies are utilized responsibly and ethically.

CONCLUSION:

In a nutshell the emerging risks of Artificial Intelligence in the age of digital era and the legal accountability shredding the emergency light on grey areas of legal framework. There is no doubt that AI's lifting the people life in terms convenience, affordability, more fully ease the work which helps to have the balancing relationship in everywhere. It impacted the many industries and profession including Weather and climate, medical and health care services, banking, education and transportation which is necessary for human survival. But at the same time, it is necessary to advocate for robust law to combat the crime against the abuse of the algorithm-based applications in order to protect the human rights.

However, we say India is a developing country and its population and literacy rate was quite complex to enact and enforce the law is not easy as it seems in other countries, it requires lot of effort, money, man force and depth research about both national and international empirical based legal frame works. But at the same time India's lethargic attitude towards delaying the process of enacting rules to enforce Digital Data Protection Act,2023 is highly objectionable cause without law that clearly prohibiting, that still considers as legal, which puts the data under threat.

Corporate criminal liability and international cooperation are essential for governing AI in a complex global landscape. Holding companies accountable for the misuse of AI technologies ensures that organizations implement robust safeguards and ethical practices. This approach addresses the potential for AI to be used in criminal activities, promoting responsibility and preventing harm. International cooperation, facilitated by entities like the United Nations and the OECD, is crucial for creating harmonized regulations. By working together, countries can tackle cross-border challenges such as data privacy, AI bias, and misuse, ensuring that AI benefits are shared globally while mitigating risks. Balancing

[60] Rogue replicants: Criminal exploitation of deepfakes in South East Asia | Global Initiative
[61] An AI tool used in thousands of criminal cases is facing legal challenges (nbcnews.com)
[62] Ibid 55

corporate accountability with global collaboration fosters a fair and secure AI ecosystem.

Private law enforcement plays a crucial role in this ecosystem by providing individuals and organizations with the means to seek redress and hold wrongdoers accountable. Legal remedies such as compensatory damages, restitution, and injunctive relief ensure that victims are compensated for their losses and that harmful activities are stopped. Furthermore, legal frameworks must adapt to address AI-specific issues, such as bias and discrimination, privacy violations, and accountability for autonomous systems. Strengthening these frameworks will enhance the overall effectiveness of AI governance, making sure that technology serves the public good while respecting individual rights. In essence, a well-rounded AI ecosystem that integrates strong private law enforcement and legal remedies not only promotes innovation but also ensures justice and fairness in the age of AI.

SUGGESTIONS:

To effectively deal with the multitude of issues confronting artificial intelligence (AI), a thorough legal framework is required.

- This framework should clearly identify the roles and obligations of all parties involved in AI development, deployment, and use, assuring accountability at all levels. For example, developers must guarantee that their algorithms do not perpetuate prejudices, as seen by the contentious usage of flawed predictive police systems in the United States.
- Transparency and explainability are crucial; AI systems should be required to use explicit and intelligible decision-making procedures. This criterion is critical in industries like as healthcare, where AI's participation in diagnostic conclusions must be visible in order to maintain patient confidence and safety.
- Data protection and privacy should align with global standards such as the General Data Protection Regulation (GDPR), ensuring that personal data is securely handled. Like Singapore, Election Commission in India may consider prohibiting deepfakes and other digitally modified information from candidates during elections. Like USA, Clarifying Lawful Overseas Use of Data (CLOUD) Act may be enacted to address the cross-border issues in favour of the country.
- Rigorous testing for bias and fairness in AI systems is necessary to prevent discrimination. For example, facial recognition systems must undergo extensive validation to avoid racial and gender biases, as evidenced by several studies showing these systems' higher error rates for non-white individuals.
- Human oversight mechanisms are essential to intervene when AI systems malfunction or are misused. This principle is critical in autonomous vehicles, where human intervention can prevent accidents caused by system failures. Audit trails and continuous monitoring protocols should be implemented to trace AI decisions and actions, thereby aiding in accountability and investigation.
- Corporate criminal liability must be enforced to hold organizations accountable for inadequate safeguards, promoting ethical AI practices. The Volkswagen emissions scandal serves as a reminder of the necessity for stringent corporate accountability in technology deployment.