# AI AND CRIME IN THE NEW DIGITAL ERA: NAVIGATING CHALLENGES AND LEGAL RESPONSES IN INDIA

Mr. Kapil Kodak[1] & Dr. Rishikesh Singh Faujdar[2]

**ABSTRACT**

The emergence of artificial intelligence (AI) has transformed number of fields, including law enforcement and criminal justice. In India, the integration of AI technologies presents unique challenges and opportunities in addressing crime in the new digital era. Examining how AI can enhance crime prevention and detection while also raising ethical concerns regarding privacy, bias, and accountability. Furthermore, the study analyzes India's current legal framework and the necessity for policy reforms to effectively regulate AI in crime prevention and enforcement.

Through the use of case studies, this study seeks to offer a thorough grasp o f how to strike a balance between protecting civil rights and using AI for pu blic safety in a society that is becoming more and more digital.

To effectively manage the difficulties of AI and crime in India, policymakers, engineers, and human rights activists must work together, according to the results.

**Keywords:** Artificial Intelligence, criminal justice, challenges and opportunities, crime cybercrime, ethical prevention, civil rights, lawmakers, navigate.

[1] Research Scholar Departrment of Law Nagaland University, Lumami Nagaland
[2] Assistant Professor Department of Law Nagaland University Lumami, Nagaland

## Introduction

In the current digital era, artificial intelligence (AI) is a disruptive force that is altering almost every aspect of human life. AI technologies are accelerating innovation at a rate never seen before in a variety of industries, including banking, healthcare, and communication. Although AI has many positive effects, there is a negative aspect to this revolution as well. Together with the complexity of AI systems, criminals' methods for exploiting them are also become more sophisticated. AI is not only revolutionising industries but also changing the criminal scene by bringing in a new era of complicated criminal activities and magnified traditional crimes.

The use of artificial intelligence-driven technology for cybercrime, such as identity theft, hacking, and data breaches, is growing quickly. Furthermore, the rise of deepfake technologies, AI-generated phishing schemes, and automated ransomware attacks is testing law enforcement's capacity to stay up. These crimes are more efficient and difficult to track down, as AI may function autonomously, obscuring the source of attacks. Machine learning algorithms have made it possible for criminals to alter data, get beyond security measures, and carry out illegal actions more accurately and extensively than in the past.

One of the key features of AI is its ability to learn and adapt, this presents particular difficulties for the legal and regulatory frameworks designed to combat crime. Criminals leveraging AI can adapt their methods in real time, evolving faster than traditional law enforcement techniques can respond. This has created a new frontier in the fight against crime, where the tools and strategies that once sufficed are now becoming obsolete. The growing ubiquity of AI in both public and private sectors has led to concerns about the absence of preparedness in dealing with AI-related crimes, leaving vulnerabilities that could be exploited by bad actors.

At the same time, AI itself is being used by law enforcement agencies to prevent and combat crime. Predictive policing algorithms, AI-powered surveillance systems, Using the aid of machine learning techniques to identify patterns of criminal behaviour, predict potential threats, and improve crime detection rates. But using AI in the law enforcement raises complex ethical and legal enquiries, such as privacy issues, bias, and accountability. For instance, predictive policing has drawn criticism for promoting systemic biases, as these algorithms

often rely on evidence from the past that might indicate discriminatory practices, thereby perpetuating inequality in law enforcement.

The evolving nature of AI crime furthermore needs a rethinking of Regulation and law approaches. Current legal frameworks were not designed with AI in mind, and consequently, there are notable gaps in how AI-related crimes are prosecuted and regulated. Questions surrounding liability, accountability, and the legal status of AI systems are becoming increasingly urgent. For example, if an AI system commits a crime autonomously, who is held responsible? Is it the developer, the user, or the AI itself? Such questions challenge traditional legal notions of culpability and require innovative legal responses that can address the complexities of AI-driven crimes.

Furthermore, international cooperation is essential in tackling AI-related crime, as these crimes often transcend borders. The worldwide aspect of the digital era means that Cybercriminals are able to operate from any location worldwide, making it challenging for any one country to effectively combat AI-enabled crimes on its own. International legal frameworks and cross-border collaborations will be crucial in developing comprehensive strategies to address these challenges.

This article aims to provide an in-depth exploration of AI and crime in the new digital era, focusing on the unique challenges that AI-driven technologies present for law enforcement and the legal system. It will also analyze the current legal responses to AI-related crimes and propose ways in which the law can evolve to better address the ethical, practical, and regulatory complexities of this rapidly changing landscape. As we navigate the intersection crime eith the AI, it is imperative to achieve equilibrium between leveraging AI's potential for societal good and protecting individuals and institutions from its misuse. Only by use of a proactive and adaptive legal approach how can we be sure that the benefits of AI are realized without compromising security, justice, and ethical standards.

**AI-Driven Crime: Emerging Threats in India**

As AI technology progresses at a rapid pace in India, its use in illegal activities has become a significant problem in the legal field. The convergence of AI and crime has led to a new generation of criminals who use AI algorithms to do complex cybercrimes, hackings, and other illegal acts. One of the most critical difficulties confronting the legal system is the

detection and attribution of AI-driven crimes.[3] Criminals use AI-based evasion strategies and anonymizing technologies, which makes it difficult for law enforcement to track down the attackers or determine where the attacks originated. Because the issue of liability and accountability gets very difficult when addressing its autonomous and ostensibly self-directed AI algorithms, the legal uncertainty surrounding AI's involvement in criminal actions exacerbates the situation. Artificial intelligence is being employed to help doctors diagnose patients more rapidly and accurately. Its algorithms could examine medical imaging such as MRIs, CT scans, and X-rays to find anomalies and help with early disease identification.[4] AI is assisting in the creation of individualized treatment programs for individuals by examining their medical background and genetic composition. This may result in less harmful treatments that are more successful.[5] The COVID-19 pandemic has hastened the implementation of telemedicine in India, with AI helping to make remote consultations more successful. AI-powered diagnostic tools and remote monitoring systems were employed to provide care to patients from afar.[6] AI is helping medical research by identifying patterns and trends in large datasets that might lead to improvements in disease knowledge and therapy. [7] AI is becoming increasingly important in the search and development of new drugs. It might speed up the drug development process by analysing large datasets to find and forecast the efficacy of possible therapeutic candidates.[8] In such circumstances, while doctors or inventors may not want to injure someone, if AI makes an incorrect choice due to negligence, it may result in an offence. This is because negligence regarded as one of the elements of *mens rea*.[9]

The growing use of AI in criminal operations has far-reaching consequences for data privacy and security in India. Criminals are using AI algorithms to collect and misuse personal data, jeopardising people's privacy and safety. With the growing reliance on artificial

[3] Margetts, H. (2022). Rethinking AI for good governance. Daedalus, 151(2), 360–371. https://www.jstor.org/stable/48662048 https://doi.org/10.1162/daed_a_01922

[4] Puttagunta, M., & Ravi, S. (2021). Medical image analysis based on deep learning approach. Multimedia Tools and Applications, 80(16), 24365–24398. https://doi.org/10.1007/s11042-021-10707-4

[5] King, M. R. (2023). The future of AI in medicine: A perspective from a Chatbot. Annals of Biomedical Engineering, 51(2), 291–295. https://doi.org/10.1007/s10439-022-03121-w

[6] Bokolo, A. (2021). Exploring the adoption of telemedicine and virtual software for care of outpatients during and after COVID-19 pandemic. Irish Journal of Medical Science, 190(1), 1–10. https://doi.org/10.1007/s11845-020-02299-z

[7] Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: Management, analysis and future prospects. Journal of Big Data, 6(1), 54. https://doi.org/10.1186/s40537-019-0217-0

[8] 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

[9] Baron, M. (2020). Negligence, men's rea, and what we want the element of mens rea to provide. Criminal Law and Philosophy, 14(1), 69–13. https://doi.org/10.1007/s11572-019-09509-5

intelligence across a variety of industries, the risk of data breaches and unauthorised access to sensitive information is a major worry.

Another important feature of AI's engagement in criminal activity is its ability to increase societal disparities and prejudices in the justice system. AI algorithms employed in predictive police and law enforcement may unintentionally reinforce preexisting prejudices, resulting in disproportionate targeting of specific communities or individuals. This might lead to violations of civil and human rights, necessitating a thorough evaluation and control of AI application in the legal realm.

AI is seen as a paradigm-shifting technology owing to the numerous useful strategies that have been demonstrated in recent years, the majority of which are credited to a subfield of AI known as "deep learning".[10] The creation of novel works such as texts, paintings, films, and self-driving cars are only a few instances of the interdisciplinary and broad areas in which tangible applications have been demonstrated recently. Other examples include intelligent robots, human-level spoken interaction, superhuman performance in games, self-driving cars, and intelligent robots. Images, text, and sounds can be produced or modified in a highly realistic manner by utilising the advanced potential of deep learning.[11] As a result, Deep Learning has enabled the creation of fake texts, fake sounds, fake films, and fake photographs that appear to be authentic and lifelike at first glance. Such technological skills have the ability to change digital media, but their societal repercussions might be severe, undermining confidence of the people in what is seen, heard, and eventually accepted to be true. Several well-known deepfakes circulate the Internet and can be found on famous websites like YouTube. The 2018 video of Barack Obama is among the first and most well-known deepfakes[12] wherein, ironically, he sends out a warning against the perils of deepfakes—something Obama never really accomplished. Some other deepfakes are celebrity porn videos, as well as a misrepresentation of politicians e.g., replacing the face of Angela Merkel's with Donald Trump's, or Donald Trump's with that of Mr. Bean. Other deepfakes include celebrity pornography and political persona misrepresentations, such as using Donald Trump's visage instead of Angela Merkel's or Mr. Bean's face instead of Trump's. Deepfakes can create original

[10] R. Chesney and D. Citron, "Deepfakes and the new disinformation war: The coming age of post-truth geopolitics." Foreign Affairs, vol. 98, no. 1, pp. 147–153, 2019.
[11] M. Westerlund, "The emergence of deepfake technology: A review," Technology Innovation Management Review, vol. 9, no. 11, pp. 39–52, Jan. 2019.
[12] ] "You Won't Believe What Obama Says In This Video," YouTube, 2018. [Online]. Available: https://www.youtube.com/watch?v=cQ54GDm1eL0

content in addition to superimposing images within videos. Even better, users may utilise the available software to instantly generate deepfake avatars for Zoom and Skype teleconferencing applications by only taking a picture.[13] Similar technology (deep learning) has the potential to produce fake CVs[14]. While it may still seem like a "innocent" playground to some, imagine the following scenarios: either the human resources department of a large company is inundated with realistic-looking resumes and photos of prospective hires, or there are phoney users posing as other people in real time during business teleconferences (where most people conduct business during the COVID19 pandemic). Deepfakes are simple to generate, even for home users, and don't require extensive technical knowledge because to the technology's minimal learning curve and public accessibility. This may result in the production of realistic-looking phoney information, whose veracity may be difficult to ascertain. In conjunction with social media dissemination, this could intensify already-existing fake news campaigns. Deepfakes have previously been applied in real-world situations; they don't constitute a "someday, this might be possible" technology. The capacity to fabricate images and, occasionally, videos is not a novel concept; nevertheless, how simple it is to accomplished it and the resulting realism are both novel and concerning.

Digital platforms, especially social media, is closely linked to deepfakes as it allows them to spread to a large audience. Its effects on the public realm are profound because text, images, videos, and sound are the fundamental components of contact and communication there. Even if the potential and strength of AI are still being explored and are far from being regulated, reports of these efforts in the media present a variety of perspectives, with the implications ranging from the apocalyptic end of the human race to the keystone of its continued existence. The relationship between digital media and artificial intelligence (AI) is fascinating because it unites the fundamentals of contemporary media communication with the most recent advancements in AI technology, which erode boundaries between reality and information sharing. As a result, there might be an unprecedented increase in the impact of digital media, which could both positively and negatively impact society. It could also be abused to sway public opinion. "The ability to distort reality has taken an exponential leap

[13] "Avatarify: Avatars for Zoom, Skype and other video-conferencing apps," GitHub, 2020. [Online]. Available: https://github.com/alievk/ avatarify

[14] "This resume does not exist," website, 2019. [Online]. Available: https://thisresumedoesnotexist.com

forward" in the case of deepfakes.[15].

The emergence of automated financial crimes represents another domain in which the application of AI presents noteworthy legal obstacles. Financial system flaws and vulnerabilities can be found by criminals using AI algorithms, which makes money laundering, fraud, and other illegal financial operations easier.[16] Technology speeds up and simplifies financial analysis and decision-making with the use of computers and AI-powered tools. The application of AI systems in trading, which makes transactions happen "with lightning speed"[17] has both favourable and unfavourable aspects. In terms of positive aspects, the current financial technology has, for instance, decreased transactional charges and costs of capital for businesses.[18] However, algorithmic trading with decisions that are difficult to follow for humans inserts instability into the market. As a result, a risk for highspeed crashes (i.e., flash crashes) emerges.

**Legal Responses: Indian Legislation and Regulatory Framework**

India currently lacks specific laws directly addressing generative AI, deepfakes, and AI-related crimes, although the authorities have said relevant legislation is in the works. Currently, there are several laws that provide both criminal and civil remedies. For example, deepfake offences pertaining to privacy violations are covered under Section 66E of the Information Technology Act, 2000, and are punishable by three years in jail, maximum or a fine of INR 200,000. Malicious use of computers or communication devices is the focus of Section 66D, which carries fines and/or jail time as punishment. Furthermore, publishing or sending obscene deepfakes may be prosecuted under Sections 67, 67A, and 67B of the IT Act. Social media agencies are necessary by the IT Rules to quickly remove such content; failing to do so could result in the loss of "safe harbour" protection.

Further recourse for deepfake-related cybercrimes is provided by the Bharatiya Nyay Sanhita (previously known as the Indian Penal Code) under Sections 196 and 197 (spreading hate on communal lines), Section 356 of the Sanhita (criminal defamation), and Section 79

[15] R. Chesney and D. K. Citron, "Deep fakes: A looming challenge for privacy, democracy, and national security," SSRN Electronic Journal, 2018.
[16] Seth, S. (2017). Machine learning and artificial intelligence: Interactions with the right to privacy. Economic and Political Weekly, 52(51), 66–70. http://www.jstor.org/stable/26698381.
[17] . Scopino, Algo Bots and the Law: Technology, Automation, and the Regulation of Futures and Other Derivatives. Cambridge, U.K.: Cambridge Univ. Press, 2020.
[18] T. C. W. Lin, ''The new market manipulation,'' Emory Law J., vol. 66, pp. 1253–1314, Jul. 2017.

(insulting modesty of a woman). Notably, Section 51 of the Copyright Act of 1957 forbids the unapproved use of copyrighted material to create deepfakes, and can handle cases involving this kind of activity. Furthermore, recent examples show how law enforcement applies provisions relevant to forgeries in deepfake events. AIFORALL, the first national AI plan, was introduced by Niti Ayog in 2018 to promote artificial intelligence inclusively. The plan listed agriculture, smart cities, healthcare, education, and transportation as key sectors for national priority in AI innovation and implementation. Since then, some of the strategy's suggestions have been put into practice, including the creation of cybersecurity and data protection regulations as well as the creation of top-notch datasets to support research and innovation.

The National Artificial Intelligence Strategy was followed by the creation of The Guidelines for Ethics in AI by NITI Aayog in February 2021. Under the headings of system and societal considerations, this document examines moral dilemmas pertaining to AI application solutions in India. The effects of automation on job opportunities and job creation is the main focus of societal issues, whereas system considerations mainly deal with decision-making principles, equitable beneficiary participation, as well as responsibility.

The second section of the ethical guidelines for AI, which focusses on implementing the ideas generated from the ethical issues examined in the first part, was released by NITI Aayog in August 2021. In conjunction with the corporate sector and research organisations, the statement emphasises the importance of government involvement in encouraging responsible AI application in social sectors. It emphasises the need for capacity building, regulatory and policy activities, and the promotion of moral behaviour by fostering an ethical mindset around AI among private organisations.

On August 11, 2023, the President of India officially signed the Digital Personal Data Protection Act, 2023. This Act, which takes effect right away, controls how digital personal data is processed in India, regardless of how it was originally stored. It has the potential to address some of the privacy concerns associated with AI platforms.

Under the Information Technology Act of 2000, the Indian government released the Information Technology Rules (Intermediary Guidelines and Digital Media Ethics Code), 2021 (IT Rules 2021), which provide a framework for managing a number of organisations, such as digital news media, OTT platforms, and social media intermediaries. These rules became in force on May 26, 2021, and they were revised on April 6, 2023.

The National Data Governance Framework Policy (NDGFP) draft was released by the Ministry of Electronics and Information Technology (MEITY) on May 26, 2022. This policy's objective is to improve and modernise government data management and gathering practices. The primary objective of the NDGFP, according to the plan, is to establish an extensive dataset repository in order to promote an atmosphere in India that encourages startups and AI/data-driven research. Committees on AI have been established by the Ministry of Electronics and Information Technology, with the objective of providing reports on the advancement of AI, safety issues, and ethical considerations. In a similar vein, the Bureau of Indian Standards, which functions as the country's national standards agency, established an AI group that is currently formulating draft Indian standards in the area.

**Judicial Pronouncements on AI-Related Crimes**

The Information Technology Act, 2000 (often known as the "IT Act") and the Rules enacted under it make up India's legislative foundation for cyber law. The main piece of law that defines different types of cybercrimes, the penalties that can be applied, the requirements that intermediaries must follow, and other things is the IT Act. However, the IT Act's provisions are not the only ones that make up the Indian Cyber Law framework. India's Cyber Law framework has undergone substantial modification as a result of several verdicts. To fully understand the scope of the Cyber Law regime, the following important Cyber Law cases in India must be reviewed:

**Shreya Singhal v. UOI[19]**

The Supreme Court heard a challenge to the legality of Section 66A of the IT Act in the present case.

Information: Following the death of a political leader, two ladies were detained under Section 66A of the IT Act for posting comments on Facebook that were deemed indecent and undesirable. The IT Act's Section 66A penalises anyone who uses a computer resource or communication to disseminate information that is derogatory, inaccurate, or that incites annoyance, discomfort, danger, insult, hostility, hurt, or malice. After the arrest, the women

[19] (2013) 12 SCC 73

filed a petition alleging that Section 66A of the IT Act violates their right to free speech and expression, thereby making it unconstitutional.

Decision: The three ideas of discussion, advocacy, and incitement served as the foundation for the Supreme Court's ruling. The observation made was that the essence of freedom of speech and expression lies in the simple act of discussing or even advocating for a cause, regardless of its unpopularity. It was discovered that Section 66A could impose restrictions on all types of communication and that it failed to differentiate between speech that is merely offensive advocacy or discussion of a cause and speech that is intentionally provocative and links public disorder, security, health, and other issues. The Court responded to the inquiry of whether Section 66A seeks to shield people from defamation by stating that it forbids insulting remarks that might irritate a person but do not harm his reputation. Nonetheless, Additionally, the Court noted that because there was a discernible distinction between material conveyed via the internet and through other channels of communication, Section 66A of the IT Act did not violate Article 14 of the Indian Constitution. Furthermore, the claim of procedural unreasonableness was not even addressed by the Apex Court due to its substantive unconstitutionality.

**Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anr.[20]**

Facts: Under the Dhirubhai Ambani Pioneer Scheme, the subscriber selected a Reliance phone and Reliance mobile services. The user desired to go to a different service provider due to their being drawn to their superior tariff plans. The Electronic Serial Number, or "ESN," was compromised by the petitioners, who were TATA Indicom employees. Reliance phones' Mobile Identification Numbers (MIN) were permanently linked with ESN; as a result, the device would be verified by the petitioner's service provider rather than Reliance Infocom after ESN was reprogrammed.

Questions before the Court:

i) Is a phone under the definition of a "computer" under Section 2(1)(i) of the IT Act?

ii) Does changing an ESN that is preprogrammed into a mobile phone qualify as changing the

[20] 2005 CriLJ 4314

source code for the purposes of Section 65 of the IT Act?

Decision: (i) The IT Act's Section 2(1)(i) defines a "computer" as any fast data processing system or device that can be optical, magnetic, electrical, or another type. Additionally, it encompasses any computer software, input, output, processing, storage, and communication facilities that are linked to or associated with the computer inside a computer system or computer network. Through the manipulation of electrical, magnetic, or optical signals, computers carry out arithmetic, logical, and memory operations. Consequently, a phone handset is considered a "computer" under Section 2(1)(i) of the IT Act.

(ii) Through ESN alteration, other service providers such as TATA Indicomm can use exclusively used devices. Because each service provider is required to keep its own SID code and assign a unique number to each device used by its clients to access the services, altering an ESN is therefore illegal under Section 65 of the IT Act. Accordingly, Section 65 of the IT Act does not allow for the offence against the petitioners to be revoked.

**Christian Louboutin SAS v. Nakul Bajaj & Ors**.[21]

Facts: A luxury shoe manufacturer filed a lawsuit against www.darveys.com, an online marketplace, alleging trademark infringement by the seller of counterfeit goods, and asking for an injunction. The defendant sought protection under Section 79 of the IT Act for its application of the plaintiff's mark, logos, and picture. It was the question put to the court.

Decision: Due to the website's complete control over the goods sold on its platform, the Court observed that the defendant is not only a middleman. It finds third parties and then encourages them to market their goods. The Court went on to state that an e-commerce platform that actively participates would not be subject to the rights granted to intermediaries under Section 79 of the IT Act.

**Avnish Bajaj v. State (NCT) of Delhi** [22]

Facts: The CEO of Bazee.com, Avnish Bajaj, was detained for transmitting cyber pornography in accordance with Section 67 of the IT Act. Via the bazee.com website, another

[21] (2018) 253 DLT 728
[22] (2008) 150 DLT 769

person had sold copies of a CD that contained sexual material.

Decision: The Court observed that Mr. Bajaj had no involvement whatsoever in the transmission of any pornographic content. Furthermore, the Bazee.com website did not allow users to view the sexual content. However, Bazee.com is paid for running advertisements on its website and gets a commission from sales.

The Court further noted that the information gathered implies that a person apart from Bazee.com is responsible for the cyberpornography violation. Mr. Bajaj was granted bail by the court, contingent upon the provision of two sureties, each worth Rs. 1 lakh. But the onus is on the accused to prove he was only a service provider and didn't create the content

This case is noteworthy in the Cyber Law regime since it resulted in a conviction in less than seven months from the FIR filing date.

Facts: The accused was a close friend of the victim's family and wished to wed her, but she wed another guy, leading to a divorce. The accused tried to convince her once more after her divorce, and when she refused to marry him, he used the Internet to harass her. Under the victim's name, the accused created a phoney email account and posted offensive, offensive, and defamatory content against the victim.

Sections 469 and 509 of the Indian Penal Code, 1860 (now Bharatiya Nyay Sanhita) and Section 67 of the IT Act served as the foundation for the charge sheet brought against the defendant.

Decision: The accused was convicted by the Additional Chief Metropolitan Magistrate, Egmore, in accordance with Sections 67 of the IT Act and 469 and 509 of the Indian Penal Code, 1860. The defendant was fined Rs. 500 under Section 469 of the Indian Penal Code. The defendant was fined Rs. 500 under Section 509 of the IPC. The culprit was sentenced to two years of harsh imprisonment and a fine of Rs. 4,000 under Section 67 of the IT Act.

**SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra**[23]

Facts: In this instance, the plaintiff's business employed the defendant, Jogesh Kwatra.

[23] CM APPL. No. 33474 of 2016

To disparage the business and its managing director, Mr. R K Malhotra, he began sending nasty, abusive, offensive, and filthy email correspondence with his bosses and many branches of the aforementioned company across the globe. The email was discovered to have originated from a Cyber Cafe in New Delhi during the investigations. During the investigation, the Cybercafé employee recognised the defendant. Plaintiff terminated Defendant's services on May 11, 2011.

Decision: Currently known as Bharatiya Sakshya Adhiniyam (BSA), Section 65B of the Indian Evidence Act does not qualify the court's decision as certified evidence, so the plaintiffs are not entitled to the remedy of a perpetual injunction that they have prayed for. The lack of tangible evidence that the defendant was the sender of these emails prevented the court from accepting even the strongest evidence. Additionally, the defendant was ordered by the court not to publish or transmit any disparaging or abusive content about the plaintiffs online.

**Challenges and Gaps in Indian Law**

There is debate in India over the application of AI and what it means for its users. To avoid discriminatory practices and stigmatisation, it is essential that these systems in the Indian context are made to represent the country's diverse people. The intricate social dynamics, demographics, cultural variety, and historical background of India compound the challenges in creating optimal AI model prototypes that meet the requirements of the heterogeneous populace. Artificial intelligence (AI)-enabled devices are developing quickly, and frequently without the developers considering or assessing the biases or harms they might unintentionally be feeding into the AI models. thereby producing discriminatory effects and a breach of basic rights. Similar to this, India's AI development and application processes lack accountability and transparency.

Furthermore, there is a growing risk of civil liberties violations and invasions of personal privacy due to instances of government and corporate actors abusing AI technology. There are significant security concerns with the usage of AI in facial recognition technologies, tracking people, and other forms of surveillance and monitoring. As AI technology develops, personal data is being collected indiscriminately and could be altered at the whim of the data controller, putting people in dangerous situations. However, as there are no underlying criteria in India's Artificial Intelligence Act, it will be interesting to observe how the act identifies a high risk AI system given the country's unique issues and circumstances.

Furthermore, jobs involving regular tasks are expected to be replaced by AI-driven automation, which might cause unemployment to rise at an unprecedented rate. Furthermore, this could lead to less financial stability, especially for the groups in society who are more prone to be marginalised. AI is already widely used in many sectors of the economy, including banking, education, healthcare, and science. While there is no denying that AI has brought about revolutionary advances, it is crucial to consider both the impact on people's livelihoods and the true efficiency of this technology. The digital gap may worsen if people heavily rely on technology without fully understanding its impacts.

Another risk that AI presents is social manipulation through algorithmic systems. This has caused a great deal of disinformation to circulate, rumours to flourish, and users to develop strange prejudices. This issue has become worse by deepfakes, speech manipulation, AI-generated audiovisuals, etc. Anyone may now easily control huge audiences via social media in a matter of minutes thanks to AI. News consumers now question the authenticity and reliability of the content due to this. With the countless other challenges, these are just a handful of the pressing issues that must be prioritised in order to enhance AI governance.

**Proposed solutions for the AI crisis**

It is crucial to remember that artificial intelligence (AI) has several drawbacks, including the use of facial recognition, surveillance systems, and autonomous weapons. These damages then have a substantial effect on basic rights like the right to privacy and other rights. Clearly defined laws and regulations must be established in order to address each of these issues. Laws and regulations must also include the special characteristics of India's AI industry. To lessen the threats that new technologies pose to democratic principles and basic rights, governments and the courts would need to establish clear regulations and supervision processes.

Furthermore, there need to be improvements made to the judiciary's and governments' capacity to understand, assess, and regulate AI systems. Simultaneously, the government needs to acknowledge and enhance its capacities in order to comprehend, evaluate, and oversee artificial intelligence. Furthermore, the government would need to make more investments in order to construct better infrastructure. Expertise is also required to support efficient governance and oversight of the AI ecosystem. This could entail setting up an impartial agency to oversee AI in addition to allocating funds and other resources for AI system audits, testing, and development. Regulations should also contain clauses that prohibit the government and

business sector from abusing artificial intelligence, particularly in regard to conducting criminal investigations. In addition, it will be crucial to discuss the specific behaviours AI forbids. One source of inspiration for implementing the same is Article 5 of the EU's AI Act, which lists a number of detrimental practices, including the use of subliminal techniques that operate outside of a person's conscious awareness.

The government can work to improve infrastructure and human resources to reduce misuse and other unfavourable effects related to AI solutions. This could entail putting in place an efficient organisational structure, HR procedures that satisfy the demands of both employees and clients, and worker training resources. A much-needed step will be the creation of a new, independent organisation to supervise the application of AI, provide funding for research and development and testing, and oversee and audit these activities.

To address these issues and prevent the risks of misuse of AI technologies by the government or by private companies—such as with regard to vigilantism through surveillance, predictive policing, and the exploitation of vulnerable groups—it is also evident that the industry needs to be regulated through a variety of means. While the Digital Personal Data Protection Act of 2023 deserves praise, a more complete legislative framework is required. Data manageability techniques and privacy regulations must be developed in order to safeguard individual rights. Based on multiple research, it is anticipated that by 2024, the use of mental health in medical procedures will reach a record high.

India has to prioritise developing the skilled labour force necessary to properly manage, employ, and govern the development of AI if it is to become a centre for innovation and industry. The ethical use of any technology that we introduce into society must be prioritised above everything else. This calls for placing more focus on education, training, and capacity building for the purpose of providing the skills required to handle the problems relating to AI that India's plan must address.

## Conclusion

Notwithstanding the fact that India has significant progress in regulating AI, the government's current rules are attacked for being dated and ephemeral. However, regulations seem to require a more sophisticated, along with a more driven framework, for the purpose of properly minimise the harm that comes with proactive usage and inclusion of AI. To achieve

this, strict policies and procedures must be developed, as well as autonomous oversight organisations and strong regulatory authorities. For agencies to properly assess and oversee the wide range of AI applications, they need to be outfitted with improved knowledge, pertinent credentials, and proficiencies. Creating a robust code of ethics that can guard against algorithmic bias, preserve privacy, and guarantee openness in the development, application, and application of AI is a major need. Even though India has made several initial steps in this regard, more specific and thorough regulatory action is required. In addition to helping us better take advantage of AI's advantages, a practical and all-encompassing framework would act as a safety net against any unforeseen challenges in the road.

In the digital age, artificial intelligence (AI) offers India both prospects and challenges. Artificial intelligence (AI) can be used to improve security and fight crime, but It may also result in new and sophisticated types of criminal activity. India's legal system has to change to meet the special difficulties brought on by crimes involving artificial intelligence, such as algorithmic fraud and deepfake technology. Collaboration between policymakers, regulators, and the court is necessary to develop a comprehensive legal framework that balances technological innovation with the demands of security, privacy, and accountability.

The ability of India to create flexible and adaptable legal frameworks, implement global best methods, and ensure that the advantages of AI are realised without sacrificing justice and public safety will determine how AI and crime develop in that nation. India can only successfully handle the intricacies of AI and crime in the new digital era by taking such a comprehensive strategy.

**References:**

1. Adv. Mali.P. Ph.D.,Addressing the Challenges Posed by AI in India, DNLU-SLJ, < https://dnluslj.in/addressing-the-challenges-posed-by-ai-in-india/> accessed 10 October 2024.

2. "Avatarify: Avatars for Zoom, Skype and other video-conferencing apps," GitHub, 2020. [Online]. Available: https://github.com/alievk/ avatarify

3. Bokolo, A. (2021). Exploring the adoption of telemedicine and virtual software for care of outpatients during and after COVID-19 pandemic. Irish Journal of Medical Science, 190(1), 1–10. https://doi.org/10.1007/s11845-020-02299-z

4. "Crime in India – 2019" Snapshots (States/UTs), NCRB, *available* at: https://ncrb.gov.in/sites/default/files/CII%202019%20SNAPSHOTS%20STATES.pdf (Last visited on 5th Oct; 2024)

5. Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: Management, analysis and future prospects. Journal of Big Data, 6(1), 54. https://doi.org/10.1186/s40537-019-0217-0

6. King, M. R. (2023). The future of AI in medicine: A perspective from a Chatbot. Annals of Biomedical Engineering, 51(2), 291–295. https://doi.org/10.1007/s10439-022-03121-w

7. Margetts, H. (2022). Rethinking AI for good governance. Daedalus, 151(2), 360–371. https://www.jstor.org/ stable/48662048 https://doi.org/10.1162/daed_a_01922

8. Puttagunta, M., & Ravi, S. (2021). Medical image analysis based on deep learning approach. Multimedia Tools and Applications, 80(16), 24365–24398. https://doi.org/10.1007/s11042-021-10707-4

9. R. Chesney and D. K. Citron, "Deep fakes: A looming challenge for privacy, democracy, and national security," SSRN Electronic Journal, 2018.

10. Scopino, Algo Bots and the Law: Technology, Automation, and the Regulation of Futures and Other Derivatives. Cambridge, U.K.: Cambridge Univ. Press, 2020.

11. Seth, S. (2017). Machine learning and artificial intelligence: Interactions with the right to privacy. Economic and Political Weekly, 52(51), 66–70. http://www.jstor.org/stable/26698381.

12. T. C. W. Lin, ‘‘The new market manipulation,’’ Emory Law J., vol. 66, pp. 1253–1314, Jul. 2017.

13. “This resume does not exist,” website, 2019. [Online]. Available: https://thisresumedoesnotexist.com