VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

REGULATING AI-GENERATED DEEPFAKES IN INDIA: LEGAL GAPS AND THE NEED FOR A DEDICATED CRIMINAL FRAMEWORK

- Chirag Narwat[1]

Abstract

The word "deepfake" is a portmanteau of "deep learning" and "fake" (Rouse,2020).It refers to a type of artificial intelligence (AI) technology that incorporates a machine learning technique called generative adversarial networks (GANs) (Rouse, 2020). GANs was first introduced in 2014 by Ian Goodfellow and other researchers at the University of Montreal . The idea is to use a pair of neural networks – one of which is called the "generator," and the other, the "discriminator" – to synthesize artificial media or multimedia content that is indistinguishable from its authentic counterpart (Brownlee, 2019). One of the most striking features of this algorithmic architecture is its ability to use as little as one image of a person tocreatea videoclipofthatpersonsayingordoingthingstheyneversaidordidinreallife[1]. In recent years, deepfake technology has earned its reputation as a threat to our already vulnerable information ecosystem (Schwartz, 2018). Until late 2017, the use of this machine learning technique was mostly confined to the area of AIresearch (Schwartz, 2018). It was onlywhenaReddituserwho,underthemoniker"Deepfakes,"beganpostingdigitallyaltered pornographicvideosinwhichcelebrities'faceswereSuperimposedontothebodiesofwomen in pornographic movies, that this technology became widely known in the public domain (Schwartz,2018).BythetimeRedditlaterbannedthepostinganddisseminationofdeepfakes from its platform, the creator of the videos had released "FakeApp," an easy-to-use platform for making forged media. With the help of FakeApp, deepfake technology became widely knownandavailabletothepublic,resultinginadramaticincreaseinthenumberofindividuals who utilized this technology to generate and disseminate deepfakes online, mainly through social media platforms. In September 2019, the AI firm Deeptrace found approximately 15,000 deepfake videos online, 96% of which werepornographic.

[1] Student at Amity University, Noida

Introduction

2.1 INTRODUCTION

The ability of the government to ensure efficient, effective, transparent, and responsive administration is essential to governance, which is widely defined as the "activity or manner of managing a state." Given the size and diversity of India, governing it presents particularly difficult challenges. Government in India has always been constrained by slow, out-of-date procedures and bureaucratic obstacles, but recent efforts to integrate newer technologies are giving the system new life. To this end, there has been ongoing discussion in recent years on how to best employ AI to promote effective governance.

Three major trends came to light during the analysis made in this research. First, while interest in the idea of applying algorithms across all states has been high, technological capabilities and implementation vary widely. In adopting the use of algorithms in industries like education and agriculture, Andhra Pradesh and Karnataka appear to be more aggressive than other states. Second, the commercial sector, which collaborates with the government through partnerships or contracts, is responsible for developing the majority of the AI technology that is currently in use. And last, much of the technology that is at the center of discussions about AI and governance in India has already been put into practice in other nations, especially the United States, the United Kingdom, and China. Even if India might try to adopt some of this technology, it would be a good idea to first analyze some of the technological, legal, and ethical issues that have emerged in these nations and find ways to overcome them before implementing the technology in Indian administration. In order to chart the trajectory of technology development in India in the near future and make a regulatory model readily available after the technology is in use, this paper, unlike the other case studies, pays a significant lot of attention to uses of AI in other jurisdictions.

2.2 SECTORS INCORPORATING AI USE IN INDIA

Key AI technologies are being researched and in some circumstances are being deployed by law enforcement on a global scale which includes drones, robocops, autonomous police cars, voice recognition, facial recognition, and predictive analytics, too. Our research in this area revealed that India's technical development is still in its infancy. Many initiatives are still in the ideation stage and lack the proficiency to completely integrate AI solutions for law enforcement.At the same time, India is working on initiatives that will provide the data and infrastructure required to power AI solutions in the field of law enforcement. Important applications of AI in Indian law enforcement include:

A. Predictive Analysis

India has made progress in using big data analytics and algorithms to handle enormous amounts of data in order to create predictive police models.[383] Predictive policing technologies are expected to be accessible in five states by March 2018: Kerala, Odisha, Maharashtra, Haryana, and Tripura. By the end of 2018, it is anticipated that this technology will be available in all 50 states. Running predictive police programmes requires the use of improved and sophisticated data collection methods. The National Crime Records Bureau is reportedly collaborating with Hyderabad-based Advanced Data Research Institute (ADRIN) to create the technology necessary to implement predictive policing techniques.

Police officials have made a compelling case for the employment of predictive policing techniques, and effective measures are being done in all states to establish reliable data collection procedures. The National Crime Records Bureau held a workshop on data analytics, dashboarding, and the application of artificial intelligence in policing in May 2017. The importance of evidence-based predictive policing tactics was underscored by N. Ramachandran, President of the Indian Police Foundation, who also emphasized that India should strive to become a global leader in predictive policing. The Special Commissioner of Delhi Police discussed the necessity of fusing control room data and social media applications with CCTV footage during the event. A tendency in state initiatives has been toward broader and finer-grained data collecting that could help AI solutions. One such instance is the 30,000 CCTV cameras that the Telangana Police are said to have installed with community assistance. With funding from the National e-Governance plan, the Crime and Criminal Tracking Network and Systems were launched in India in 2013. The project's goal was to integrate roughly 15,000 police stations, district and state police headquarters, and automated services to create a national criminal tracking database. It has the potential to make it easier to collect the quantity, quality, and type of data required for predictive policing, despite having been initially planned to be finished by 2012.

In order to facilitate criminal identification registration, monitoring, and missing persons searches, law enforcement in Rajasthan commissioned a pilot project with Staqu, an AI startup, in 2017. The project's goal was to develop the application ABHED (artificial intelligence based human efface detection). The application makes use of machine learning and is meant to facilitate integration with the CCTNS.According to EtihsamZaidi, a senior analyst at Gartner, the move toward predictive policing may be influenced by the fact that the Indian police force now has more access to established data storage platforms like Hadoop and NoSQL, which allow for the immediate storage and processing of enormous amounts of incoming data.

According to Balsingh Rajput, superintendent of police (SP) cyber for Maharashtra, the police force is creating predictive methods. Using cutting-edge technology and data mining, they are attempting to predict criminal intent. Additionally, he told Hindustan Times that "Predictive Policing would change how policing is carried out in the future. We are developing tools that will help foresee issues with law and order, map out crime, and provide solid information about the motives of offenders before a crime is committed.

The Indian Space Research Organization and the Delhi Police have begun collaborating on predictive policing techniques (ISRO). The Crime Mapping, Analytics and Predictive System is a system that is in the works that will provide police officers access to real-time information at crime scenes, easing the strain of having to return to police stations to complete reports. The web-based software is able to gather information from the Dial 100 hotline of the Delhi Police and employs clustering algorithms to detect 'hotspots' spatially using satellite imagery from ISRO. Thus, similar to PredPol, this software enables Delhi Police to anticipate when and where crime may occur and subsequently deploy police troops to make strategic interventions. At the moment, crime mapping is performed every 15 days.

The Joint Commissioners prepare the reports, which they then forward to the Special Commissioners, who then send them on to the police chiefs. They then employ three techniques to process the information at hand and carry out their surveillance operations. A "crime prediction" is the first tactic, which would allow the police to spot gangs in certain regions in real-time. This system processes and analyses petabytes of data from a dozen crime databases as part of a project known as the Enterprise Information Integration Solution (EI2S). The second method is called "neighborhood analysis," which essentially involves grouping hotspots using algorithmic evaluation of geospatial data.

A third method called proximity analysis would make it possible to evaluate information about suspects, victims, witnesses, and other people who were situated close to the scene of the crime and utilize that information to analyze any changes that had occurred soon before or after the event.[393] With the assistance of IIM Ranchi, the Jharkhand police department is likewise attempting to establish a data analytics system. The method is built on the use of complex algorithms and behavioral science, which will help forecast crime, especially in Naxal-prone areas. In India, the effectiveness of predictive police techniques has not yet been evaluated.

B. Speech and Facial recognition

A partnership was recently established between Best Group and the Israeli security and AI research firm Cortica to analyze the terabytes of data streamed from CCTV cameras installed in public spaces. Improving safety in public spaces like streets, bus stops, and train stations is a

key goal of this project. The Punjab Artificial Intelligence System (PAIS), which digitizes criminal records and automates research through features like facial recognition, was developed by the Punjab Officers in collaboration with Staqu. By using facial recognition, police may get information about the offender. If a police officer finds a suspect, he snaps a photo of him. The photo is next entered into the phone app, which compares the digital image with the previously stored photo. Additionally, the app will quickly convey the individual's criminal history to the concerned officer's phone.

H-Bots Robotics, a Hyderabad-based technological start-up, has created a smart policing robot that has not yet been used in the field. The "robocop" can help maintain law and order and improve traffic control. If it were to be deployed autonomously, it might perform a wide range of crucial security-related tasks, such as preserving security at strategic intersections in locations like malls and airports.

C. Education

According to our research, decision-making, student services, monitoring student progress, and personalized learning are where AI is most commonly employed in education. Despite the wide variety of languages spoken in India, it doesn't seem like many of the solutions being created in this field have a language focus. The most frequently used method among the solutions appears to be machine learning.

1.Decision making- HTC Global Services, a US-based service provider, is concentrating on the introduction of products in the Indian educational market. Students will be able to make better choices while selecting courses and electives at colleges thanks to this web-based tool. This application will effectively employ the same algorithms that let users choose products on e-commerce sites by using AI and machine learning to analyze historical data.

2.Student Service- This would include answers to difficulties like admissions questions, which are primarily manual and take a lot of time—from the perspective of both students and professors. Vishal Sethi, Global Practice Head for AI & Data Science, has stated that they are preparing to introduce an algorithm that can accurately interpret students' facial expressions to determine their level of knowledge.

3.Student Progress Monitoring- In order to enable personalized monitoring of children and provide individualized attention to their progress, the Chandrababu Naidu-led government in Andhra Pradesh is aiming to gather information from a variety of databases and process the data through Microsoft's Machine Learning Platform. This will help reduce school dropouts.

4.Personalized Learning- An open-source learning tool called Ek-step makes use of APIs (API). The platform makes use of gamified appsthat may be found on Google Play. As of 2016,

it was purportedly used in more than 10,000 government schools in Karnataka. Additionally, the platform is accessible in 18 states and 5 languages. Co-Impact, a grouping of the world's top philanthropists that includes the Rockefeller Foundation and the Bill and Melinda Gates Foundation, recently announced that it will soon begin working with the EkStep Foundation. To spread the platform across the nation, the government also intends to collaborate with EkStep.According to CEO Shankar Maruwada, this project can be scaled up in the future even if for now, only teachers will need a mobile phone or IoT device to access the content. Using artificial intelligence to organise and filter pertinent content for each individual learner would undoubtedly be advantageous for such a project. It might either develop into a smart content platform that serves as a teaching tool or be employed to create an ITS model using the current platform.

D. Defence-

Our study revealed that AI is mostly used in the defence industry for intelligence, surveillance, and reconnaissance, robot soldiers, cyber defence, risk terrain analysis, and intelligent weapons systems. Defense is the only industry we examined where the employment of autonomous systems is explicitly being considered. However, a lot of these initiatives are still in the planning and experimental stages, and it's unclear how much the various branches of the government actually trust and support them.

Intelligence, Surveillance and Reconnaissance- The Indian army has begun to employ unmanned autonomous vehicles for reconnaissance tasks like spotting naval mines in littoral areas and keeping watch over territorial waters to look for intruders. To undertake airborne reconnaissance and surveillance, a variety of unmanned aerial vehicles have also been created, such as the recently tested Rustom-248, which can operate in both manual and autonomous mode. Daksh is a robot created by the DRDO that can be controlled remotely within a 500-meter range. Its main function is to spread explosives, much to PackBot, which is utilised by the US army. The development of this technology has also been aided by collaborations with the private sector. As an illustration, Crone Systems, a New Delhi-based AI business, has examined seasonal data for signs of border infiltration and can algorithmically predict the likelihood border crossings at specific periods. Innefu Labs is collaborating with the Border Security Force and Central Reserve Police Force to monitor social media posts in order to predict the location and timing of unrest and dispatch the necessary people.

• Robot Soldiers- DRDO-affiliated laboratory, the Centre for Artificial Intelligence and Robotics (CAIR), has been working on a project to create a Multi Agent Robotics Framework (MARF). This aims to inspire the development of a variety of robots that can cooperate and work as a team, much like human troops, through the use of multi-layered AI-powered architecture. Robots that have already been constructed include a Robot Sentry, a Snake Robot, and a Wheeled Robot with Passive Suspension. The US wants to create unmanned and manned intelligent teaming in combat roles and autonomous convoy operations by 2025, indicating the direction of the technology and the possibility that there may be more "robot warriors" than people.

6.Cyber Defence- The use of AI by the government is enhancing and expanding cybersecurity capabilities. For instance, CDAC is working with IIT Patna on a project to create artificial intelligence (AI)-powered cyber forensic tools that may be used by law enforcement, the government, and intelligence organizations.[409] The Indian government has contracted with Innefu to analyse data from intelligence agencies to assess threat patterns and forecast future events in their most recent product, called Prophecy.

7.Risk Analysis- According to a publication from the Defense Research and Development Organization (DRDO), AI is being used in risk-terrain analysis in the following ways: (1) Military Geospatial Information System: This facilitates the creation of terrain trafficability maps (often referred to as Going Maps or GMs) in relation to five thematic layers, including soil, slope, moisture, land use, and landform. The maps are then produced in a three level hierarchical fashion after they have been combined. (2) Terrain Feature Extraction System: This system enables the classification of land uses by training a multilayer perceptron and generating various themes afterwards. (3) Terrain Reasoner System: Enables decision-makers to create alternate routes for completing a mission that has been predetermined, (4) Terrain-Matching Systems: These are intelligent aids that include intricate case-based deliberation into a unified whole.

8.Intelligent weapon System- A modified Pilotless Target[2] Aircraft (PTA) Lakshya-II that had been successfully tested for numerous rounds, according to DRDO's confirmation in February

[2] *Supra* note 404

2018, had become India's first "armed drone."According to the DRDO, it has conducted 9 successful flights with a precision of 20 meters.

2.3 CHALLENGES IN INCORPORATION OF ARTIFICIAL INGTELLIGENCE IN INDIA

India's socioeconomic, technological, and regulatory realities present particular challenges that must be acknowledged and taken into account when formulating policy and implementing the technology, despite the country's great potential for the advancement of artificial intelligence in the governance sector.

• ***Improved capacity and enhanced understanding of emerging technologies***-To effectively adopt AI-driven solutions, the government must increase its capabilities. This would also require more openness to, knowledge of, and skill with information technologies—qualities that the people in charge of putting the solution into action, such as teachers, police officers, or government officials, may not have. Given that the development of AI-driven solutions for governance is mostly being pursued through collaborations with the private sector, a significant portion of this capacity building may need to come from the private sector. The developer working with the private sector, the government body adopting the technology, and the government official or individual implementing the solution at the community level must all maintain open channels of communication in order to build capacity.

• ***Infrastructure***- According to our research, the necessary infrastructure has not yet been created for the successful and coordinated implementation of AI-driven solutions. For the purpose of developing algorithmic models that accurately capture the wide range of socio-economic realities in India that would need to be employed in predictive policing models, the inputs that may be used as training data in the law enforcement sector are not coherent or diverse enough. Infrastructure challenges in the field of education include a lack of internet connection and IoT device availability. In India as a whole, 31% of people have access to the internet as of 2016. Out of 444 million people, 269 million in urban India utilise the internet (or 60% of the population), whereas just 163 million[3] in rural India use the service (17% of the population, according to the 2011 census). The then defence minister NirmalaSitharaman has identified the absence of a sufficient technology infrastructure as a major barrier to the deployment of AI in the sector.

[3] M.J. Philomina, & S. Amutha, "Information and communication technology awareness among teacher educators" 6*International Journal of Information and Education Technology*, 603 (2018).

• ***Trust-*** Genuine worries about potential cultural ambiguity arise from each society that has grown accustomed to employing conventional tools rather than algorithmic models, especially intelligent models, across sectors. Locally employed police officers and educators have obtained training and practical experience utilising methods unrelated to the usage of AI or knowledge derived from it. In many instances, their training and experience don't even involve the usage of ICTs. Despite being enthusiastic about the strategic advantages of building autonomous solutions, the operational units of the defence forces do not entirely trust the CAIR-developed solutions.

• ***Funding-*** In the modern day, finding funding to build AI-driven solutions is a difficulty for any expanding economy. By allocating Rs. 3,037 crores to the "Digital India Programme" in the 2018 budget, the government has once again demonstrated its support for the creation of AI-based solutions. This is done in an effort to increase funding and skill sets in the fields of robotics, artificial intelligence, and the Internet of Things (IoT). Under the direction of NITI Aayog, there has been some emphasis on creating a National Artificial Intelligence Program. International Centers for the Transformation of Artificial intelligence should be established, according to an NITI AAYOG report. The research suggests that, aside from the costs of the physical infrastructure and technological/computing infrastructure, seed money (in the range of INR 200 crore to INR 500 crore per ICTAI) through grants from the public and commercial sectors should cover the operational costs of the ICTAI for the first five years. Despite the fact that these are encouraging developments, it is yet unclear how financing will be allocated to various sub-sectors. Due to the ambiguity surrounding this matter, it's likely that the majority of funds is allocated to some sub-sectors that the government considers to be essential at the expense of others.

Conclusion

Within the relatively short time span of one year of writing this thesis, deepfakes havebecome more convincing and have gotten new implementations. A new app calledDeepFaceLive now allows users to replace their face with a face of someone else into livewebcam footage. Users can use this technology to enter Zoom or Skype meetings,impersonating others. I do not need to explain the potential new problems that may arise. Theunavoidable truth is that deepfakes spell trouble.