THE ETHICAL IMPLICATIONS OF USING ARTIFICIAL INTELLIGENCE IN LAW ENFORCEMENT: BALANCING EFFICIENCY AND PRIVACY CONCERNS

Ashendra Mani Pandey*

ABSTRACT

Artificial Intelligence is a lethal virus to Law enforcement or advancement towards better redressal mechanisms or in AI courts. With rising AI applications and many AI engines with different structures but mostly identical in algorithmic structuring of generating solutions, which makes it traceable and easily interpreted by offenders, which can impact transparency, privacy, and just & reasonable solutions for establishing justice and equity. This article in general is aiming at the rise in Artificial Intelligence in the past 5 years, now seeping its way into Legal Fraternity posing the same threats (as seen when corporates feared losing their jobs) with a more severe impact as Law and Order is one of the fundamental pillars in a democracy which if comes in the hand of Artificial Intelligence can be more dangerous to the entire country.

INTRODUCTION

The proliferation of artificial intelligence (AI) in different sectors has been creating many controversies and disputes it seems to also seep into the legal fraternity. Artificial intelligence is one of the tools which has an enormous and wide range of utilities that can curb time exploitation and secure justice in many ways. On July 11, 2018, there was 1st INTERPOL - United Nations (UNICRI) global meeting[1] on the opportunities and risks of artificial intelligence and Robotics for law enforcement. The following topics and areas were discovered below:

*BCOM LLB, FIFTH YEAR, DR. SHAKUNTALA MISRA NATIONAL REHABILITATION UNIVERSITY, LUCKNOW.

[1] 1st INTERPOL - United Nations (UNICRI) global meeting (1st December 2022) <www.interpol.int/News-and-Events/News/2020/Artificial-Intelligence-and-law-enforcement-challenges-and-opportunities> accessed on 25th March 2023

- How machine vision might help law enforcement agencies detect anomalies and faces[2] in security footage[3], for example. Machine vision is being applied in retail and manufacturing, and these use cases could have transferrable applications for law enforcement.
- How AI can be used to generate visual media. Programmatically-generated images and videos could allow law enforcement to falsify evidence, and it could also allow criminals to create videos of events that never happened, leading to some disturbing consequences.
- Singapore presented a demo of a robot[4] that it hopes will be able to patrol its streets in the next five years.
- Some countries have reasonably advanced AI applications in law enforcement today. That said, it's not a regular part of policing yet in any country[5].
- There seems to be a burgeoning ecosystem of AI vendors in the law enforcement market. There was a demo room at the summit where many vendors offered machine vision and drone technology[6].
- INTERPOL as an organization seems to be waking up to AI as a relevant tool, and they're investing in educational initiatives to teach law enforcement agencies about the possibility space of AI. INTERPOL is launching a technology radar, including a library of AI use cases[7].

There are many studies goings-on and some are already reported out of which one recent study that examined the relationship between artificial intelligence (AI) and law enforcement gave an outcome with both the need for law enforcement agencies (Executionary bodies acting at district levels) to be involved in the development of public policies regarding AI – such as regulations, governing autonomous vehicles (in US), cross-checking or verifying pieces of evidence, – and the need for law enforcement officers to better understand the limitations and ethical challenges of AI technologies. "Law enforcement agencies have a crucial role to play

[2] Facial Recognition in Law Enforcement-6 Current Applications, <emerj.com/ai-sector-overviews/facial-recognition-in-law-enforcement/> accessed on 25th March 2023
[3] AI for physical security – for current applications, <emerj.com/ai-sector-overviews/ai-for-physical-security/> accessed on 25th March 2023
[4] law enforcement robotics and drones – 5 current applications, <emerj.com/ai-sector-overviews/law-enforcement-robotics-and-drones/> accessed on 26th March 2023
[5] Daniel Faggella Presented at a United Nations- INTERPOL Conference on AI in law enforcement, <emerj.com/emerj-team-updates/dan-presented-at-a-united-nations-interpol-conference-on-ai-in-law-enforcement/> accessed on 26th March 2023
[6] Ibid
[7] Ibid

in implementing public policies related to AI technologies[8]", says Veljko Dubljević, corresponding author of the study and an associate professor of science, technology, and society at North Carolina State University.

EFFECT OF AI IN IDENTIFYING CRIMINAL BEHAVIOUR

As we know AI has not come out of the blue it needs data and research[9]. Singapore Police has used the help of Robocops[10], a type of robot that is used on tracks especially roads on daily routines with a specific time and path pattern which makes it very efficient and cost-effective in patrolling at night. AI in criminal cases or cases which are severe in nature has a lot of potentials which can many courts, use facial recognition, and check whether evidence is produced not digitally made (such as videos and photos). We have seen a lot of CCTV cameras that are attached to Traffic Lights for better monitoring and maintaining traffic rules for the safety of the citizens (from an Indian perspective). These cameras can be integrated with an AI facial recognition engine which can help identify malpractices on roadways, identifying the person (who is accused of any offense) who either ran away or are yet to be caught or are on the run, but, these type of technology is there in India but it still needs to implemented nationwide with multiple servers at least at the level of capital cities linked with other cities of the states, for easy tackling criminal activity all over the state which can be lead under an IPS Officer or DM for strict monitoring and action taking. In parallel, many jobs will be created and many opportunities for different streams. In a joint INTERPOL-UN conference on AI in law enforcement[11], "According to the US Government Accountability Office[12], the Federal Bureau of Investigation's database contains over 30 million mugshots of criminals and ID card images from 16 states[13]. This is just one of many law enforcement databases which also contain further identity information, including fingerprints and text data, with needs to improve investigation times and streamline the task of matching suspect images within a pool of numerous identities, government officials, law enforcement offices, and commercial vendors

[8] Study Highlights Complicated Relationship Between AI And Law Enforcement, <news.ncsu.edu/2023/03/ai-and-law-enforcement/> accessed on 22 March 2023
[9] CHATGPT and environmental research by Jun-Jie Zhu, Jinyue Jiang, Meiqi Yang, and Zhiyong Jason Ren, <https://doi.org/10.1021/acs.est.3c01818> accessed on 28 March 2023
[10] "Singapore has deployed robot police officers to discipline citizens". The danger is the cop inside people's head- Editorial *The Indian Express* (October 7, 2021)
[11] Daniel Faggella Presented at a United Nations- INTERPOL Conference on AI in law enforcement, <emerj.com/emerj-team-updates/dan-presented-at-a-united-nations-interpol-conference-on-ai-in-law-enforcement/> accessed on 26th March 2023
[12] FACE RECOGNITION TECHNOLOGY: FBI should better ensure privacy and accuracy [reissued on August 3, 2016], <www.gao.gov/products/gao-16-267>
[13] Facial Recognition in Law Enforcement-6 Current Applications, <emerj.com/ai-sector-overviews/facial-recognition-in-law-enforcement/> accessed on 25th March 2023

are researching how AI, specifically computer vision, can be used to improve facial recognition[14].

At Interpol 2020 – UNICRI Global Meeting[15], Speakers reported their work and said "Through our research, we aim to show insights on how various law enforcement agencies and companies are implementing facial recognition technologies.

Speakers spoke about the challenges and opportunities of AI in law enforcement[16]

[Above stated image is subject to copyright which is owned exclusively by the 1st INTERPOL - United Nations (UNICRI) global meeting (1st December 2022)[17], Above image, is used for learning and teaching purposes under the fair use, Author of this article doesn't own any of the information provided above in the image]

This research will be broken up into the following two categories:

[14] Facial Recognition Applications – Security, Retail, and Beyond, <emerj.com/ai-sector-overviews/facial-recognition-applications/> accessed on 27th March 2023
[15] 1st INTERPOL - United Nations (UNICRI) global meeting (1st December 2022) <www.interpol.int/News-and-Events/News/2020/Artificial-Intelligence-and-law-enforcement-challenges-and-opportunities> accessed on 25th March 2023
[16] Ibid
[17] Ibid

- **Government and Law Enforcement Applications:** Law enforcement agencies and government organizations that have implemented facial recognition software.
- **Commercial Vendor Applications:** Vendors that claim to offer facial recognition solutions to law enforcement or security-related organizations.

The UNICRI report and this article address[18] some of the important questions below:

1. What are the benefits of integrating AI into law enforcement?
2. What can law enforcement do to forecast and mitigate the weaponization of AI and robotics?
3. How can law enforcement successfully implement certain use cases of AI and robotics in the real world?
4. How can AI systems have used in policing the balance between privacy and security?
5. Why should the ethical usage of AI be categorized and enforced in law enforcement as a frame of reference for other domains and industries?

I would also need to highlight some of the research and use case graphics from **Emerge**[19] it clearly stated how there are several potentially useful use case scenarios concerning AI applications in law enforcement, the report uses the same 4 broad categories, combined with criteria about the relative majority of the application as given below:

DEVELOPEMNT STAGE / CATEGORY OF USE				
CONCEPT	▸ Analysis of Text-based Intelligence ▸ Enhancing Fairness in Investigations	▸ Vehicle Identification ▸ Video and Audio Analysis		
PROTOTYPE	▸ Agent-Based Simulation ▸ Prediction of Protests and Crime ▸ Contextual Analysis of Intelligence	▸ Information Extraction for Online Crime Reports ▸ Face and Soft Biometrics ▸ Identification of Child Pornography	▸ Audio Translation	▸ Perimeter Patrol Robots
EVALUATION	▸ Predictive Policing ▸ Digital Forensics System ▸ Identification of Suspicious Behaviour ▸ The Incredible Machine	▸ Audio and Visual Analysis for Prisons ▸ Statement-taking Machine ▸ Voice Analysis for Telecommunications ▸ Surveillance Systems for Criminality	▸ Communication Robots	▸ Patrol Drones for Prisons and Borders ▸ Surveillance Drones ▸ AI-generated Patrol Live Stream
APPROVED FOR USE	▸ Identification of Legally Privileged Information ▸ Crime Anticipation			

[18] Artificial Intelligence in Policing – Use Cases, Ethical Concerns, And Trends (16 December 2019), <emerj.com/ai-sector-overviews/artificial-intelligence-in-policing/> accessed on 25th March 2023.
[19] Ibid

[Above stated image is subject to copyright which is owned exclusively by Emerge under the article Artificial Intelligence in Policing – Use Cases, Ethical Concerns, And Trends (16 December 2019)[20], Above image, is used for learning and teaching purposes under the fair use, Author of this article doesn't own any of the information provided above in the graphic chart]

AI IN POLICING (International Reference)

As we have seen above police are employing and utilizing AI in different types of their daily patrolling commodities. Further, AI has a lot of advantages as they help the text threat in many large gatherings such as parades, festivals, or sporting events, law enforcement agencies can deploy technology to keep a watchful eye over the crowd and detect threats. In India, we have Yearly and Quarterly very large auspicious events, festivals, and gatherings with some major religious gatherings also, police departments can use AI-enhanced image and video technology to help with crowd control and surveillance of certain heavily populated areas as AI-enabled computer vision systems can assist officers in public spaces such as sports venues, train stations, and airports, providing constant surveillance. One of the greatest examples can be seen in the category of facial recognition technology, especially in China[21]. It was seen that; Chinese authorities have identified and painted out individual criminals among thousands of people in Stadium with the help of facial recognition technology. Guiyang, China is one of the examples which can be put forward as the city has a network of over 10,000 cameras throughout the city to help police identify and arrest the suspects. One of the private companies in China Hikvision is innovating and building cameras with built-in deep neural networks. With the help of these AI and neural network camera as they can very prudently detect suspicious anomalies in crowded areas such as unattended bags or an out of place cars, likewise, many AI-enabled cameras in India can keep an eye out for suspicious activity for all hours of the day even in extreme temperature areas which can be also monitored inside a suitable comfortable environment for more efficient tracking and constant surveillance.

AI-enabled drones can also help in border surveillance and monitoring suspicious activities, and also save many lives of our soldiers, similarly, AI-enabled remote-controlled robots can be used at night patrolling.

[20]Artificial Intelligence in Policing – Use Cases, Ethical Concerns, And Trends (16 December 2019), <emerj.com/ai-sector-overviews/artificial-intelligence-in-policing/> accessed on 25th March 2023.
[21] Countries Need National Strategy for AI To Stay Competitive-ED Burns (tech target, 20 November 2018), <www.techtarget.com/searchenterpriseai/feature/Countries-need-national-strategy-for-AI-to-stay-competitive> accessed on 28th March 2023.

ARTIFICIAL INTELLIGENCE (AI) WITH THE QUALITIES OF LAWYERS AND JUDGES[22]

High-profile police violence and discrimination[23] exacerbate an already skeptical public who are generally dissatisfied with AI, creating a barrier to developing ethical debates in the surveillance of AI technology[24]. However, this study builds on previous studies examining the ethical implications of AI by identifying the most important law enforcement qualities for police officers, to expand the research on AI morality and characterization of virtuous police[25]. Responsible AI incorporates the virtues of honesty, honesty, loyalty, and compassion into the design of non-human agencies, reducing suspicion and giving them the appearance of competence in such law enforcement applications. Moreover, as technology advances, AI can incrementally improve the reliability and performance[26] of police practices[27] (Foreign Reference). Artificial intelligence technology has the potential, at least in principle, to support the moral judgments that emerge in situations where police officers need to make split-second decisions with greater accuracy and precision. For example, there are parallel efforts involving rational decision-making in the application of big data and artificial intelligence in the medical field to improve the accuracy of medical protocols[28]. Similarly, the increased reliability and power of AI technologies compared to their human police counterparts will reduce resistance to implementing these technologies in the community, leading to conflicting and negative feelings may decrease[29]. Its benefits create socially desirable AI policing technologies as public

[22] Exploring And Understanding Law Enforcement's Relationship with Technology: A Qualitative under the Study of Police Officers in North Carolina <www.mdpi.com/2076-3417/13/6/3887#B24-applsci-13-03887> accessed on 28th March 2023.
[23] #Black Lives Matter surges on Twitter after George Floyd's Death, (Pew Research Centre, June 10, 2020), <www.pewresearch.org/fact-tank/2020/06/10/blacklivesmatter-surges-on-twitter-after-george-floyds-death/> accessed on 28th March 2023.
[24] Ouchchy, L., Coin, A. & Dubljević, V. AI in the headlines: the portrayal of the ethical issues of artificial intelligence in the media. *AI & Soc* 35, 927–936 (2020) <https://doi.org/10.1007/s00146-020-00965-5> accessed on 28th March 2023.
[25] Daniel B. Shank, Mallory North, Carson Arnold, and Patrick Gamez –'Can Mind Perception Explain What Was Character Judgements of Artificial Intelligence?' (30 June, 2021), <assets.pubpub.org/96li91kj/01628801922123.pdf> accessed on 28th March 2023.
[26] The predictable policing: new technology, old bias, and future resistance in big data surveillance
[27] Carly E. Cortright, Wesley McCann, Dale Willits, Craig Hemmens, and Mary K. Stohr - An Analysis Of State Statutes Regarding The Role Of Law Enforcement (2020), <journals.sagepub.com/doi/pdf/10.1177/0887403418806562> accessed on 28th March 2023.
[28] Hun-Sung Kim- decision-making in artificial intelligence: Is It Always, Correct? (20 November 2019), <synapse.koreamed.org/articles/1140257> accessed on 28th March 2023.
[29] Yochanan E. Bigman, Kurt Gray- People Averse To Machines Making Moral Decisions (11 August 2018), <www.sciencedirect.com/science/article/abs/pii/S0010027718302087> accessed on 28th March 2023.

safety goods, reduce the stigma of law enforcement sociotechnical expansion, and encourage community engagement.

THE ETHICS OF AI IN LAW ENFORCEMENT: BALANCING EFFICIENCY AND PRIVACY CONCERNS

Artificial Intelligence (AI) has many ethical considerations as much as it is unique and unprecedented also it brings many challenges such as privacy, bias, discrimination, economic power, and fairness. I'll be starting with a few basic concerns over data privacy and security. As already described above in this article, AI brings many extraordinary, exceptional, and defined solutions with more creativity and uniqueness but all of that comes from data which is the essence and core brain of an AI. Machine learning is a concept where multiple guitars are faded to some machine model which processes data and gives sets of different outputs depending upon the targeted question and the need of the user likewise machine learning in different AI scenarios and sectors requires large bulk and an enormous amount of data for processing and training purposes which subsequently raises questions. There have been many instances where it was seen that AI has such capabilities about patent protection that it can also make pores privacy risks even if the AI has no direct access to personal data. A study by Jernigan and Mistress where an AI can identify sexual orientation from Facebook friendships. The issue here comes when an individual's sexuality in digital traces is unintentionally leaked which is a cause of worry, especially for those who may not want this information out in the public domain. Similarly, machine learning capabilities also have the potential for the reidentification of anonymized personal data[30]. The biggest risk lies with private organizations in how they collect and process vast amounts of user data in bulk in their AI-based system machine learning and training without customer knowledge or consent, also which are anonymous data no one knows where the status is coming from and what type of status is generally the processed resulting in serious social consequences.

[30] Melanie Lefkowitz-artificial intelligence may put private data at risk (August 2, 2018), <news.cornell.edu/stories/2018/08/artificial-intelligence-may-put-private-data-risk#:~:text=Machine%20learning%20–%20a%20form%20of%20artificial%20intelligence,other%20malicious%20attacks%2C%20Cornell%20Tech%20researchers%20have%20found.> accessed on 28th March 2023.

DATA AS A COMMODITY

Data as a commodity is nowadays considered because earlier data was an asset[31] for a company that was helping in its business activities and helping corporates to achieve greater heights on improvising the feedback and data they have collected over some time from its customers or consumers. But today data must be processed to be able to provide benefits and advantages, similar to the raw material that must be processed first to become finished goods that can be enjoyed by consumers. Any machine learning and data processing models its data is a very essential and one of the fundamental cores or in layman's terms can be called a soul for AI.

ETHICAL CONCERNS WITH AI OVER BIAS AND DISCRIMINATION

Technology is man-made and since the creator is human, we can interpret that either intentionally or inadvertently, will involve some kind of bias. It is well said that technology can be as good or bad as the people who develop it. In AI machine learning systems can result in the production of existing bias which in the legal field can damage the procedural aspect and following the pattern and professionalism of ML (Machine Learning) can hamper the independence and transparency of the legal fraternity. In 2014 there was a team of software engineers at Amazon building a program to review resumes and realized that the system discriminated against women[32] for technical roles.

Empirical evidence exists when it comes to AI bias regarding demographic differentials. Research conducted by the National Institute of Standards and Technology evaluated facial recognition algorithms from around hundred developers from 189 organizations, including Microsoft, Toshiba, and Intel, and found that contemporary face recognition algorithms exhibit demographic differentials of various magnitudes, with more false positives and false negatives another example is the continent in case of legislation what in San Francisco where the use of facial recognition was voted against, as they believed AI-enabled facial recognition software was prone to errors when used on people with dark skin woman[33]. These examples are some of the thousands of which AI has failed on very severe reasoned grounds, are we open to what an AI can do in other sectors imagine what it would do and how bad it would hamper the legal

[31] JeefriAmoka-Data As A Commodity: For Data Science Professional (July 3 2020), <www.datasciencecentral.com/data-as-commodity-for-data-science-professional/>
[32] Ibid
[33] Gregory Barber- San Francisco Bans Agency use of Facial Recognition Tech (May 14 2019) <www.wired.com/?url=https%3A%2F%2Fwww.wired.com%2Fstory%2Fsan-francisco-bans-use-facial-recognition-tech%2F> accessed on 29th March 2023

fraternity because starting from the occurrence of an offense till the end of the judgment of the trial court, there are innumerable processes which can easily be tweaked or changed with slight third-party influence and can release an accused guilty of a severe offense, in support of above examples I would cite Veljko Dubljevic, the statement "It's also important to understand that AI tools are not foolproof. AI is subject to limitations and if law enforcement officials don't understand those limitations, they may place more value on the AI than is warranted - which can pose ethical challenges in itself"[34]

Where most jurisdictions have established data protection laws; evolving AI still has the potential to create unforeseen data protection risks creating new ethical concerns. On the other hand, India is still lacking a data protection law (except IT laws and some statutory common law breaches are only) in almost different for all sectors as many data breaches are seen nowadays here and forth but still very few actions under the cyber cell or cyber security is taken. India is still lacking in many aspects but also holds humongous potential by dominating the world AI market because as we know AI depends on machine learning and machine learning depends on data and data comes from the population, and India is 2nd largest populated country (soon it will be first as China's population has reached its stagnation stage) in the world which makes it beyond doubt a dormant country with untapped potential.

NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE (NITI AYOG)

NITI Aayog has formulated a structured study for AI implementation all over the nation is very appreciable and unique in our positive manner which is different from other desserts journals and articles as most of the part talks about the positive side of AI which also at the same level in law enforcement with many positive effects. Since, there are many upcoming issues threats and public concerns that AI implementation might compromise money on personal privacy, security protocol, and freedom and reveal many personal identification characters which must not be revealed in public. While the issue of ethics is 1 of the primary concerns and the biases that come with an AI system work on the data working on an algorithm that can easily be traced, and recorded in a pattern concerning largely the collection of inappropriate use of data for personal discrimination. Security issue also arises from the implications and the consequent accountability of an AI system. The diverse and highly populated country has many regulatory and societal structures which are

[34] Exploring And Understanding Law Enforcement's Relationship with Technology: A Qualitative under the Study of Police Officers in North Carolina <www.doi.org/10.3390/app13063887> accessed on 28th March 2023.

dependent on human judgment and control, thus subject to inherent biases and discrimination. Extant decision-making in individual, societal, regulatory, or even judicial is purely dependent upon human limitations of knowledge, precedent, rationale, and bias (explicit or subconscious). To overcome limitations there are some delegations of some aspects that can be given to decision-making algorithms, which subsequently be able to ingest and process many more parameters as compared to a human, which may likely result in systems with reduced bias, discrimination, and improved privacy protection. NITI Ayog said "Even if a technological intervention helps us delegate that responsibility to an algorithm with improved outcomes, it is extremely important that we set much higher standards for privacy and protection in the case of AI tools[35].

ISSUE OF FAIRNESS/BIASES

AI is largely dependent upon data which is a set of well-diversified, may be an inaccurate description of the world, but the developer community takes a technocratic attitude that data-driven decision-making is good and algorithms are neutral. This is not enough to justify biases in the AI system, since the issue of fairness is still at stake and at the forefront of the discussion, as a hot topic and area of concern for other fields, as well as to the Legal fraternity for academic, research and policy forums which can bring a sustainable future and cover our concerns. I would like to quote a statement by the NITI AYOG report "One possible way to approach this would be to identify the in-built biases and assess their impact, and in turn, find ways to reduce the bias. This reactive approach, use-case based, may help till the time we find techniques to bring neutrality to data feeding AI solutions, or build AI solutions that ensure neutrality despite inherent biases."[36]

TRANSPARENCY

Transparency is one of the fundamental parts of democracy and in our country, transparency is not specifically defined under any statute or Constitution but the procedural aspect of every legal process has been provided under different-to-different statutes subject to its implication but also subject to some limitations where the such concern is of national interest. In today's technology-driven world, we are dependent upon different technologies using different types of algorithms where most of the algorithm is not in the public domain and are some parts of the secret of the court operations or private entities which are offering the service. Similarly, we are still not aware of the behind the process of AI output and input we had very little or no

[35] Arnab Kumar, Punit Shukla, Aalekh Sharan and Tanay Mahindru, Dr. Avik Sarkar, Dr. Ashish Nayan and Kartikeya Asthana - in *National Strategy for Artificial Intelligence* (NITI AYOG, June 2018), 85, Para 3.
[36] Ibid

understanding of what happens in between and only the input data and results are the known factors. Many AI systems keep on improving incrementally by Reliance on the set of parameters that are with updates and's future solutions are narrowed down, with Developers' emphasis being less on how the algorithms are achieving the requisite success. However, there is a need for a clear explanation of the decision-making process which will be transparent to the set of officials who are at that stage of working which can be government officials (IAS, IPS, or other such officials as may be necessary) retired judges with the specific knowledge and Chief Justice of India so that law enforcement and judiciary are implemented in a very positive way not in a derogating way, as AI is very relied upon that has significant consequences for a large section of the population. Since here disclosure is required for the clear and transparent procedure with proper reasonable backing but not in the context of revealing code or technical disclosure – few experts in AI solutions are concerned as rebuilding such code or technical specification makes the program vulnerable and can be exploited, what needs to be balanced is transparency security and legal reasoning for AI to be properly implemented in any Law Enforcement of a country.

DATA PRIVACY ISSUES (INDIAN REFERENCE)[37]

Earlier in this article we discussed what threats are posed by AI from International Reference, now we'll go through the same from an Indian reference, we have been going through a lot of changes in our Data Protection and IT Laws and recently curbing bitcoin transactions and blockchain is a sign that Government of India is tackling the hurdles very patiently and we'll soon reach a period where AI in different sectors will be regular set very efficiently. There are further points that would like to give on dealing with privacy issues concerning NITI AYOG:

Data protection framework[38]: Justice B.N. Srikrishna Committee submitted its report and draft bill to the of Electronics and information technology on July 27, 2002. The committee was formed in August 2017 to examine issues faced by different authorities and individuals relating to data protection and recommend methods to address them at the end of the submission and drafted a data protection Bill.

[37] Arnab Kumar, Punit Shukla, Aalekh Sharan and Tanay Mahindru, Dr. Avik Sarkar, Dr. Ashish Nayan and Kartikeya Asthana - in *National Strategy for Artificial Intelligence* (NITI AYOG, June 2018).
[38] Ministry of Electronic and Information Technology, *Report Summary on a Free and Fair Digital Economy,* (28 July 2018), (para 1) <prsindia.org/files/policy/policy_committee_reports/Free%20and%20Fare%20Srikrishna%20Committee%20Report%20Summary.pdf> accessed on 30th March 2023

Fiduciary relationship[39]: The committee observed that the regulatory framework has to balance the interest of the individual about his data and the interest of the entity such use as a service provider who has access to this data. The committee also put forward the relationship between the individual and the service provider must be viewed as a fiduciary relationship[40]. This is due to the dependence of the individual on the service provider to obtain a service which makes the consumer dependent. Therefore, the service provider processing the data is under an obligation to deal fairly with the individual's data and use it for authorized purposes only.

Obligations of fiduciaries[41]: To prevent abuse of power by service providers, the law should set out their basic obligations, which will bind them to perform actions including: (i) the obligation to process data fairly and reasonably, and (ii) the obligation to give notice to the individual at the time of collecting data to various points in the interim.

Definition of personal data[42]: The Committee specified what constitutes personal information. Personal data includes data from which an individual may be identified or identifiable, either directly or indirectly. The Committee sought to distinguish personal data protection from the protection of sensitive personal data since its processing could result in greater harm to the individual which is nowadays being exploited by private companies who in their privacy policy agreement specify that they are collecting identification data rather they collect all essential data which purely gives our way of thinking take making decisions and later on manipulating by showing targeted ads. Sensitive data is related to intimate matters where there is a higher expectation of privacy (e.g., caste, religion, and sexual orientation of the individual).

Consent-based processing[43]: The Committee headlined that consent must be treated as a pre-condition for processing personal data. Such consent should be informed or meaningful that is no undue influence or any obligation imposed on the consumer of the service. Further, for certain vulnerable groups, such as children, and sensitive personal data, a data protection law

[39] Ministry of Electronic and Information Technology, *Report Summary on a Free and Fair Digital Economy*, (28 July 2018), (para 2) <prsindia.org/files/policy/policy_committee_reports/Free%20and%20Fare%20Srikrishna%20Committee%20Report%20Summary.pdf> accessed on 30th March 2023
[40] Indian Contract Act 1872, (Act No. 9 of 1872),(w.e.f. 25-04-2023), S 16(2)(a)
[41] Ministry of Electronic and Information Technology, *Report Summary on a Free and Fair Digital Economy*, (28 July 2018), (para 3) <prsindia.org/files/policy/policy_committee_reports/Free%20and%20Fare%20Srikrishna%20Committee%20Report%20Summary.pdf> accessed on 30th March 2023
[42] Ibid
[43] Ibid

must sufficiently protect their interests while considering their vulnerability, and exposure to risks online adding are final consideration of guardians/parents. Further, sensitive personal information should require the explicit consent of the individual.

Non-consensual processing[44]: The Committee also highlighted that every function entity is not required to obtain the consent of the individual in all circumstances. Therefore, separate grounds may be established for processing data without consent. The Committee identified four bases for non-consensual processing: (i) where processing is relevant for the state to discharge its welfare functions, (ii) to comply with the law or with court orders in India, (iii) when necessitated by the requirement to act promptly (to save a life, for instance), and (iv) in employment contracts, in limited situations (such, as where giving the consent requires an unreasonable effort for the employer).

Participation rights[45]: Individual rights shall be based on the principles of autonomy, self-determination, transparency, and accountability to give individuals control over their data. The Committee categorized these rights into three categories: (i) the right to access, confirm, and correction of data, (ii) the right to object to data processing, automated decision-making, and direct marketing and the right to data portability, and (iii) the right to be forgotten.

Enforcement models[46]: The Committee also recommended setting up a regulator to enforce the regulatory framework. The Authority will have the power to inquire into any violations of the data protection regime and can take action against any data fiduciary responsible for the same. The Authority may also categorize certain fiduciaries as significant data fiduciaries based on their ability to cause greater harm to individuals. Such fiduciaries will be required to undertake additional obligations.

Amendments to Other Laws[47]: The Committee noted that various allied laws are relevant in the context of data protection because they either require or authorize the processing of personal data. These laws include the Information Technology Act, of 2000[48], and the Census Act, of 1948[49]. It stated that the Bill provides minimum data protection standards for all data processing in the country. In the event of inconsistency, the standards set in the data privacy

[44] Ibid
[45] Ibid
[46] Ibid
[47] Ibid
[48] The Information Technology Act, 2000, (Act 21 of 2000), (w.e.f. 09-06-2000)
[49] The Census Act, 1948, (Act No. 37 of 1948), (w.e.f. 13-9-1976).

law will apply to the processing of data. The Committee also recommended amendments to the Aadhaar Act[50], 2016 to bolster its data protection framework.

CONCLUSION

In recent years, the Indian government has taken several initiatives to support the growth of AI in the country. The national AI strategy was launched in 2015 which means to develop a vibrant ecosystem for AI research and development in the country. As discussed above the strategy aims to focus on 5 (five) core areas healthcare, agriculture, education, smart cities, and infrastructure.

Several private players in the country are investing heavily in AI research and development. Several Indian start-ups are working on cutting-edge AI applications such as image recognition, natural language processing, and machine learning. As said earlier, India has huge potential in the AI market only push we need from the government with proper disaffection laws and the promotion of AI research and development with some incentives or tax deductions. Some of the private players that are seen in the market till the date of 30 March 2023 as; TALENTICA SOFTWARE, SPEC INDIA, SOLULAB, SIGMA DATA SYSTEMS, BrancoSoft Private Limited, and many more.

India also such as the Indian Institute of Technology (IIT), the Indian Institute of Science (IISc), and the Indian Statistical Institute (ISI), are actively engaged in AI research. Bringing in our legislation on the data protection law is a great step and 1 of the essential steps to be taken in the country which would protect individual privacy, ensure autonomy, and laud those for a smooth growing data ecosystem. This draft (Data Protection Bill) can create a free and fair Digital economy where freedom is the primary feature of individual autonomy with regard and in respect to personal data and fairness in the regulatory framework where individual rights are respected.

[50] Aadhar Act 2016, (Act No. 18 of 2016), (w.e.f. 25-03-2016)