AI in Police Work

- ***Dr. Kamal Kishore Singh, IPS, ADG***

Law enforcement is in charge of public safety, and must handle all of the challenges that come with that. Luckily, police officers are able to rely on technology for many parts of their job. In recent years, artificial intelligence in law enforcement has become an important aspect of police work globally. As AI-based police technology becomes increasingly essential to law enforcement, areas like crime prevention and prediction are going through major changes. Predictive policing is just one of the results to come out of this transformation, with other policing practices undergoing significant adjustments in the name of public safety.

Law enforcement agencies are already unlocking the potential of AI in several important ways.

1. Facial Recognition

Facial recognition technology is crucial to police departments. Police officers use facial recognition to identify criminals on the run and missing persons using image data. If you've ever seen footage from a street camera, you know how low quality these images are. As you may imagine, reviewing these images for key information is difficult and labor-intensive. Many police departments don't even have enough people or specialists to handle the volume of image analysis needed to solve all of their cases. AI in law enforcement promises greater accuracy than humans in matching faces and saves officers time. Machines can use parameters to identify faces beyond what humans can typically detect. Some AI technology today is even advanced enough to find a single face in a crowd at a stadium – something that recently helped China catch a criminal at a crowded sports event.

2. Cameras

In most major cities, cameras are everywhere on the streets and in businesses. Law enforcement often relies on this footage to review crimes after the fact and catch criminals. AI can not only apply facial recognition to these images but also identify objects and complex activities like car accidents taking place. Object identification is especially important for police officers trying to monitor large events, such as music festivals or marathons. Because they can't be in multiple places at once, officers can rely on AI in law enforcement to send an alert if someone in the area has a weapon or is acting unusually and may be a perceived threat.

Object identification has other uses as well. Through analyzing street footage, AI can identify vehicles based on set characteristics. For example, the machine could show you every blue minivan that passed through a given intersection in an hour. Where this becomes useful is when officers are looking for a stolen vehicle, or a criminal on the run, and need results quickly.

Law enforcement agencies are also working with drone cameras, which allow them to explore more surface area and engage in quicker search-and-rescue efforts. These drones are naturally equipped with AI facial and object recognition capabilities.

3. Predictive Policing

AI predictive policing refers to the ability to predict where crimes will occur, the individuals who will commit them, the types of crime, and who the victims will be. Predictive policing is a controversial topic, but it's still a long way from becoming commonplace. Companies and police departments are just starting to test out predictive policing systems. These systems could eventually provide significant strides forward in predicting and ideally preventing crimes. When it comes to predicting crime locations, algorithms can analyze crime rates across various areas and develop a map of crime hot spots. This tells police to target these areas for extra patrolling and surveillance.

AI is also able to paint a better picture of who is at risk for committing a crime, and who will likely re-offend once released from prison based on data collected and analysis of historical patterns. Naturally, there's some controversy over what should be done about this information and more debate to be had as this practice grows in use.

Where predictive policing may be most helpful is in identifying likely future victims of crimes. Research is currently being done in catching elder abuse before it happens by better understanding the environmental conditions that enable it, and using that information to project what type of abuse is most likely. While elder abuse is just one use case, imagine the implications of predictive policing in a whole other host of violent crimes as well.

4. Robots

No, we're not close to replacing our entire police force with robots anytime soon. But, police departments are turning to robots to handle tasks ranging from

the mundane to the most dangerous. Some countries are indeed testing out robots who act as replacement police officers. Dubai is experimenting with street robots that can transmit data back to headquarters to be reviewed by humans there. They're also equipped with touch screens for reporting crimes and can communicate in six different languages.

Robots can also complete more complex tasks on behalf of police officers. They can enter dangerous locations and identify humans and objects that pose potential threats, a safer alternative to risking police officer lives. There are robots that are also equipped with the ability to detonate bombs, improving public safety without putting officers in harm's way.

5. Non-violent Crimes

AI is adept at spotting anomalies in patterns, and this lends itself well to discovering non-violent crimes like fraud and money-laundering. Banks have already dived in on the AI revolution as being integral to their security, and law enforcement is partnering with these entities to catch these kinds of crimes. Through analyzing images, AI can pick out counterfeit goods and counterfeit bills with a high probability of accuracy, spotting details that the human eye may miss.

6.Pre-trial Release & Parole

AI is used in the criminal justice system during the pre-trial phase and to determine the terms of parole for an offender. These AI systems assess the risk of flight of an accused, and whether an offender should be released on parole by analyzing complex data sets. These data sets are created using historical data like crime data, as well as, personal information gathered from an individual. For instance, the US Criminal Justice System uses COMPAS (abbreviated for Correctional Offender Management Profiling for Alternative Sanctions) for basic risk assessment to determine the terms of parole for an individual. These systems assist in efficient and quick decision making in the courts of law. AI promises that the assistance it provides is more efficient than humans as this technology is free from any human errors.

Future of AI in Law Enforcement

AI may still be new to the law enforcement community, so its applications have not yet been fully realized. Nonetheless, it's already making an impact in key areas like surveillance, crime prevention, and crime-solving. With enhanced imaging technologies and object and facial recognition, AI reduces the need for labor-intensive tasks, freeing officers to handle more complex activities. AI also may capture criminals that would otherwise go free, and solve crimes that would otherwise go undetected.

Predictive policing is likewise an area to watch, as it could have major implications for how criminals are caught and how victims are identified. Ideally, predictive policing will safeguard the public even more than before, but there are still kinks to be worked out as systems become more advanced.

AI : A HUMAN RIGHTS PERSPECTIVE

The growth of AI along with implementing the technology in core areas has been so rapid that the laws have lagged behind. This technology is being created and utilized without analysing and understanding its effects on human rights. One can argue that the opaqueness and complexity of the technology have rather become a veil behind which results are given authoritative backing. Lack of digital literacy and the inability to question the results of this AI technology has raised numerous issues pertaining to human rights. AI has given a tool, so powerful, in the hands of states that total surveillance states are no more a work of fiction. The over-reliance on this technology without appropriate remedial measures has led to many human rights and technology groups demanding changes in law at the global level. These groups are working tirelessly to bring up the human rights violations that are impliedly associated with this technology. Interestingly, these violations are not nation specific but rather technology specific, and hence, one can correctly presume that if a technology is violating human rights in nation 'A', the same technology when utilized in nation 'B' will have the same results. Therefore, the need of the hour is to understand how this technology violates the fundamental human rights and what measures should be taken to tackle the same so that the benefits of the technology can be maximized. One has to understand that the implications of the use of AI in policing are vastly different due to the inherent powers of the police to detain, arrest and even use deadly force in certain circumstances.

This rationalizes the concerns being raised globally against the use of AI in policing. Unchecked AI in law enforcement can become tools in the hands of authoritarian regimes to undermine human rights, and this implies that the use of AI in policing has to be scrutinized to a higher degree as compared to any other sector. The foremost risk that AI presents is the discrimination that perpetuates due to biased algorithm. AI tech developers have always argued that as the algorithm works on data, it is beyond any human bias and thus, the results are absolutely unbiased and do not lead to any kind of discrimination. This argument has now been refuted by many international human rights and technology groups. AI inherently carries with itself the risk of perpetuating and amplifying the existing social biases. The reason behind this is the data, as AI systems are trained to analyse and then replicate the pattern that they learn from the data. Herein lays the

problem – when AI replicates the past pattern, it will inherently perpetuate the existing social biases as well. This will consequently result into what is popularly called data bias. Unfortunately, biased data is the rule rather than an exception, which leads to perpetuating and amplifying the biasness in the society. As far as AI systems that are predictive in nature are concerned, there are two kinds of such crime prediction systems at present. First, which identifies the geographical area where crimes are likely to occur. Second, which predicts individuals that are likely to commit crime. For instance, PredPol and HART predictive software used by police departments utilize historical data of past crimes and then, by analyzing the pattern, provide prediction to police. Critics argue that this data is already biased because, historically, the police is more likely to target the minority population. The biasness that is perpetuated against African-Americans in the USA can illustrate this point. The USA policing system has historically been racist, and police data show that African-Americans are more likely to be stopped by police and police is more likely to use force against them. Furthermore, African-Americans are charged and incarcerated at a higher rate as compared to the Whites. Such criminal records feed the data needs of the AI system and create a pernicious feedback loop which results in stigmatizing individuals and groups. Such neighborhoods and such individuals are now at the risk of being flagged as high risk compared to another neighborhood or individual against whom such historical data is unavailable. The effect of high incarceration and this data impacts the economic opportunities available to such groups and leads to high recidivism due to the social, cultural and economic circumstances. The criminal justice system has also started utilizing AI for pre-trial release and parole granting. COMPAS is one such AI being utilized by many courts in the US. This software again relies on the historical data and like predictive policing programs, the historical data is also biased, which in turn leads the AI to perpetuate this biasness further. ProPublica, a nonprofit investigative news reporter, found this software discriminating against the African-Americans and misclassifying them as “high risk” at twice the rate of Caucasians. It is important to note here that the criminal justice system comprising of police departments and courts is the most potent institution through which the democratic nations restrict a person’s enjoyment of human rights. AI is likely to have a positive impact in ensuring that this system is saved, from any human bias, which will also have a significant positive impact on the society as a whole. However, we have seen that the biasness of algorithms is the rule rather than an

exception and this infringes the right to equality guaranteed to every human under the International Bill of Human Rights, as well as, under the constitutions of the majority of nations. When police departments and courts are allowed to rely on the biased decisions of AI, they infringe the right of a person to be treated equally with every other citizen.

Democratic societies work on the basis of the principle 'innocent until proven guilty' but biased AI systems flag people as "high risk" due to the historical data and thereby it goes against the basic tenet of our criminal justice system. It is now being argued that the use of AI infringes the right of an accused for a free and fair trial. The AI algorithms are firstly protected under the intellectual property regime which makes it impossible for an accused to question or challenge the results. This 'black-box' paradox creates an opaque and complex system. Moreover, for these AI algorithms to work, the software have to deal in big data sets that are created using many parameters that might not have a direct correlation with the crime that one is accused of. This results in undermining the transparency and fairness in the decision making and infringement of the right to a fair trial. Furthermore, due to the 'black-box' paradox, the person relying on results of these AI tools may not even understand the basis on which the algorithm makes its decisions, which when relied upon is arbitrary. Another human right that we have secured is freedom from arbitrary arrest and detention. However, when the police or courts rely on some AI systems to analyze data and accordingly classify a person, it may be argued that, that it is arbitrary. Human Rights Watch has recently reported that China's predictive policing is enabling officials to arbitrarily detain people in Xinjiang. In a case of the Wisconsin Supreme Court in the United States, the petitioner claimed that his right to due process was violated as the court had employed the COMPAS software for risk assessment. Though the Supreme Court ruled in favor of the State, interestingly the judges held that appropriate warning needs to be given before courts employ such predictive tools. The court further concluded that "constitutional concerns required it to 'circumscribe' the use of the COMPAS risk assessment at sentencing" and stressed that "the risk scores may not be used as the determinative factor". After concerns were raised about the biasness and algorithms of these predictive tools, a sentencing commission has been formed by the Department of Justice of the United States to study the risk assessment tools and their proper role in the criminal justice system.

This leads us to another question on the accountability of such systems. Who do we hold accountable when the police or courts rely on a system that is supposed to be unbiased and works purely on data rather than any human bias or emotion? When there is an over-reliance on AI, it involves a loss of respect for human rights, fairness and transparency in name of effectiveness. With one of the worst police to person ratio in the world, AI is providing a rather miraculous solution to India. AI has made inroads in the Indian police department. Various state police are now armed with AI tools. The Rajasthan police department has tested an AI based appABHED in their criminal investigations. The Uttar Pradesh police department is now utilising the app Trinetra to track criminals. The Andhra Pradesh government has launched its AI platform e-Pragati which integrates information across the government departments. The Delhi police is now using CMAPS to identify crime hotspots. Unfortunately, if AI is implemented without providing for a procedure to establish transparency and robustness in the system, we can expect similar results in India due to the biased system. India has an opportunity to turn this nightmare operation into an effective system if it learns lessons from other nations that have failed to safeguard human rights in their jurisdiction. In the United Kingdom, the West Midlands police's ethics committee has raised concerns over privacy and implicit police bias. The project NDAS utilizes data on 'stop and search' which as noted by the ethics committee would also include information about people who were stopped but nothing was found with/on them. In the United States, investigations have proved the racial bias of the system. In China's Xinjiang, where 1.8 million Uighurs are detained, predictive tolls are used to constantly surveil the population. India is already facing privacy issues with its Aadhaar project. Furthermore, bias against scheduled tribes, scheduled castes and other minorities bog down Indian criminal system. The Andhra Pradesh government's e-Pragati is already being criticized for creating a surveillance state. India is in the phase of developing a national strategy for AI, and the experiences of other nations can help India in implementing a human rights respecting AI project.

SURVEILLANCE: NOT JUST THE LOSS OF PRIVACY

The next potent AI technology is the FRT. Around the world, countries are in the process of installing CCTVs to facilitate FRT in their territories. FRT is actively being used by the law enforcement agencies at various places and has been

deployed at the border to surveil migrants, at airports to monitor commuters, and in cities to monitor citizens. FRT aims at assisting the police to compare and identify a person based on his digital image. However, the mass surveillance program implemented by People's Republic of China through large scale use of FRT by installing CCTVs has led to many discussions over the human rights violation in China, particularly in profiling certain ethnic minorities. These claims are not unfounded as with FRT, law enforcement agencies have a tool in its hands through which it can easily monitor and profile any individual or group. These concerns have also been raised in 2019 by Special Rapporteur to the United Nations Human Rights Council. First, there are concerns about the accuracy of the technology. FRT has been proven to inaccurately identify people. An American federal study has confirmed the racial bias present in the FRT. The bias is embedded in the technology due to the lack of diversified data. This again leads to discrimination and violation of human rights.

The next concern relates to discriminatory profiling. FRT can be utilized not just to surveil but also identify and subsequently target certain communities. Such profiling, at first instance, can be a tool in the hand of an authoritarian regime to systematically discriminate against certain communities. Simultaneously, it may also interfere with the freedom of expression and freedom of association and assembly. These fundamental rights are actively utilized by citizens while expecting a reasonable level of anonymity. People may be discouraged from voicing their opinions and demonstrating or participating in any assembly due to the fear of being identified and targeted for exercising such rights. The major concern relates to the loss of privacy. The right to privacy is essential to human dignity. It includes both a legitimate expectation to respect private life as well as private data. The term 'private life' is not susceptible to an exhaustive definition but embraces multiple aspects of a person's social identity. The ease of surveillance through FRT and subsequent loss of privacy often leads to infringement of other fundamental rights such as freedom of expression and association. Implementing and utilizing of FRT leads to unreasonable searches and maybe even subsequent arrests, leading to the infringement of the right to privacy. FRT involves biometric processing of facial images. These images may be taken in public places and can subsequently be saved in databases that can be utilized later for identification purposes. Such retention and utilization of biometric data infringe

a person's right to privacy as well as the right to protect personal data. When we talk about the protection of personal data, AI systems are trained to access and analyze big data sets. FRT creates a databank of personal biometrics data without the consent of a person. This data, in the absence of stringent protection laws, can be misused by the AI systems.

Facial recognition system has already been deployed by various states in India. Punjab police department has deployed its AI powered FRT – PAIS. The Indian government has rolled out a nationwide Automated Facial Recognition System (AFRS) and the National Crime Records Bureau (NCRB) has been authorized to implement AFRS. NCRB had opened bids for private companies to develop this FRT in the country. Critics argue that this would be the world's biggest facial recognition system. Apart from concerns over privacy, this move can effectively make India, a surveillance state. It is important to note here that there has been no statute passed by the Parliament for implementing AFRS. NCRB claims that a Cabinet Note of 2009 legalizes this step but a Cabinet Note is not a law passed by the Parliament. India as of now does not have a data protection law, which makes this technology even riskier to be implemented. The Personal Data Protection bill that was introduced in the Parliament is already being heavily criticized. The bill allows the government to exempt any of its agencies from the requirements of this legislation, and allows it to decide what safeguards would apply to their use of data. These provisions will arguably constitute a new source of power for national security agencies to conduct surveillance. India already allows surveillance through various laws, such as the Indian Telegraph Act and the Information Technology Act. Deploying an intrusive technology such as AFRS will certainly increase the state of surveillance in India and infringe the right to privacy guaranteed by the Indian constitution.

SAFEGUARDING HUMAN RIGHTS

AI is a revolutionizing technology which has the potential to assist in economic as well as social growth. While it holds enormous power to benefit humanity, the technology has to be trained to respect human rights. We cannot have tunnel vision when it comes to AI and we need to be proactive to maximize the benefits of this technology while safeguarding our fundamental rights against the abuse. Contemplations for developing ethical AI have already begun. The European

Commission has issued guidelines for the development of ethical AI. The guidelines aim to promote a structure of trustworthy AI which has three components: (i) AI should be lawful (ii) AI should be ethical and (iii) AI should be robust. Although these guidelines are not legally binding, they are an important step forward. The following could be a few steps that can be taken to ensure that we safeguard human rights:

- Every nation should establish a legal framework which would carry out a human rights impact assessment on the AI system before they are developed/acquired or deployed. Along-with such assessment it should be ensured that the users are AIliterate and are be able to understand and interact with the system.
- AI systems should be deployed with human oversight. A machine should not be given the power to make decisions, and the system should always have human oversight. Human intervention and monitoring should be carried out at every stage of AI system. This will ensure that the AI systems work in a regulated framework and respect human rights.
- A comprehensive data protection legislation that can anticipate, mitigate and provide remedies for any human rights risks should be enforced. AI accesses personal data and such legislation should provide for a citizen's right to own their data and subsequent requirement for consent to access such data. The legislature has to define narrowly the legitimate purposes when such data can be accessed.
- There is a need to build a transparent information system. The public must have knowledge and information on the deployment of such systems. Furthermore, the results of such systems have to be made transparent where an individual understands how such a decision was reached and verified.
- Every person who has been impacted by any AI-related decision should have the recourse to challenge the same. This requires the nations to establish independent agencies that have the power to investigate and adjudicate such matters.
- Discrimination due to embedded biasness has to be prevented. Data diversity has to be ensured with strict non-tolerance to any AI system that perpetuates bias. Framework for due diligence should be created and human rights impact assessments should be carried out regularly.

- The UN Guiding Principles on Business and Human Rights should be implemented. These guidelines provide for businesses to prevent, address and remedy any human rights abuses committed in their operations. This would establish a structure where the private sector will be under an obligation to respect human rights and prevent their infringements. These principles will ensure the development of ethical AI.
- Lastly, there is a need to promote AI literacy. Implementation of AI without requisite AI literacy will lead to violations of human rights. Efforts must be taken to promote AI literacy in every institution utilizing AI.

There is an urgent need to assess the harm and mobilize resources towards the legal lacunae that exist in the AI ecosystem. Without due process of law, the AI systems will lead to disintegration of the human rights regime that has been built, painstakingly post the world wars. This technology creates new challenges and thus, requires immediate proactive actions by governments around the world to tackle and prevent such disintegration and make efforts for effective utilization of the technology for the betterment of humankind.

CONCLUSION

It is essential to create a safe environment for the deployment of AI and to understand the harm before implementing this technology. For instance, the European Commission is considering a temporary ban on FRT so that regulators can get time to study and work out plans to prevent the technology from being abused. The state of California has become the third state to ban facial recognition software and they have banned it for next three years to protect the right to privacy of the US citizens. Due to protests by its employees, Google has decided to not work on AI systems that could improve the target drone striking and has issued guidelines on responsible AI. These are a few positive steps and are welcomed. Big tech companies such as Google and Facebook are willing to work to develop guidelines and laws for development of ethical and legal AI. There is a need to assess the impact and bring in policies to prevent the harm that this technology could unleash on the human rights regime. The technology can and will maximize the benefits only when efforts are made to minimize the damage that this intrusive technology could create.