Deep Science Publishing
https://doi.org/10.70593/978-81-988918-1-5_12

DeepScience
Open Access Books

Chapter 12: The role of artificial intelligence in law enforcement: Surveillance, ethics, and predictive

12.1. Introduction

The introduction and integration of artificial intelligence (AI) into legal infrastructures offers tangible benefits but also problematic social consequences. Evidence-based policy has given way to algorithm-based policies, where solutions such as algorithmically-informed decision-making have helped mitigate problems like police biases and surveillance failures but also attracted equally intense criticism. The potential for the subversion of fundamental civil rights and liberties like freedom from discrimination and privacy are often invoked in this context. The integration of AI into governance processes potentially leads to systemic problems like the exacerbation of existing social inequalities based on race, ethnicity, gender, nationality, and other protected categories. For disciplines like law that traditionally predicate their findings on details and case-specific facts, the loss of transparency in how algorithms make decisions poses both moral and practical problems. AI-related decisions are typically algorithmically opaque, where even AI designers may not understand or know what goes into a model's decision. In addition, such decisions are often final, incapable of appeal to a higher authority (Garvie et al., 2016; Ferguson, 2017; Brayne, 2020). The state is seen as the driving force behind the use of AI in law enforcement, particularly in its role as regulator of the entire law development, passage, and enforcement process. Such AI development, passage, and enforcement processes inevitably privilege how states balance their responsibility to guard civil liberties and the need to uphold civil orderliness. This delineation of responsibility also shapes the responsibilities of state and private sector AI developers and manufacturers as well (Joh, 2016; Lum & Isaac, 2016).

12.2. Overview of AI Technologies in Law Enforcement

Because AI-driven technologies are being developed, validated in trials, and rushed to commercial deployment for multiple law enforcement applications, it is important to understand the variety of AI technologies that are presently available for the law enforcement domain, as well as the various tasks they are intended to accomplish. Broadly, AI-driven technology can be intended to assist human decisionmaking or to act autonomously. Some of the potential AI applications for law enforcement are, however, still embryonic and in the research stage. For many others, questions remain about how appropriately to integrate AI decisionmaking tools with human decisionmaking.

Fig 12.1: AI-Powered Surveillance and Predictive Policing

AI-driven technologies for law enforcement can help generate leads, provide intelligence for informing law enforcement investigations, automate information analysis in order to quickly surface items of interest, identify potential perpetrators, prioritize the resources committed to law enforcement, forecast when law enforcement interventions are needed, detect the presence of a crime in progress, intervene in real time to avert crime from

occurring or to prevent harm to a victim, assist in post-event investigations, intervene when a law enforcement official is in distress, deter crime, or validate a legal claim.

The research for many of these capabilities is exploratory, for example, research to improve natural language processing of unstructured text in order to automate document discovery and information analysis. Others are maturing rapidly into commercially available capabilities, such as machine vision algorithms for surveillance video analysis; predictive-policing algorithms for determining where to concentrate law enforcement presence in anticipation of crime, based on historical crime patterns; and automated license plate readers that can assist in both real-time detections of vehicles associated with threats or alerts and in post-event analysis of surveillance data.

12.3. Surveillance Technologies

Law enforcement agencies have been using several artificial intelligence techniques for many years, for instance, facial recognition and predictive policing algorithms. However, newer AI techniques, in particular deep learning, have led to a significant push towards a more aggressive use of AI in nearly all aspects of policing. Here, we will discuss some specific technologies related to surveillance and their capabilities and challenges. Surveillance is a core function of policing, with the aim of early detection of crimes, deterrence of illegal action, and collection of evidence for prosecution and conviction. Several AI capabilities are being integrated with the traditional visual and audio monitoring stages of surveillance.

Facial recognition algorithms have long been used in surveillance videos with relatively low accuracy. Deep learning has led to a step-function-like advance in biometric recognition performance, and the latest techniques are now being integrated into video surveillance systems for live verification and detection of known criminals and missing persons. While industry promotional claims for such systems may be believable, independent reviews report accuracy at the tens of percent level, particularly in incorrectly matching women or historically marginalized ethnic groups. Since accuracy is not perfect, the increasing use of such systems raises ethical and social concerns regarding invasion of privacy, incorrect matching probability, and lack of accountability. Forward-looking regulations, clear use cases, and audits for the actual usage of such systems on the ground are essential to mitigate these concerns, but such considerations are absent or overlooked in most existing facial recognition surveillance systems.

12.3.1. Facial Recognition Systems

With the unstoppable advancement of high-performance computer systems with parallel architecture, processing big data from sources like images or videos, the rising interest of institutions in deploying Facial Recognition Systems (FRSs), their comparative costs reduction associated with increased performance, and the academic interest in continuing to develop research in the area, extending results obtained on unrestricted academic datasets to real world scenarios, it can be stated that we are facing a problem that needs studying the potential dangers for the communities of the use of FRSs. This fact originates from the development of techno-scientific solutions without transparency in their use and the oblivion of the principle of precaution, which implemented in most Countries, indicates that there is a need to analyze and verify the decisions of using certain technologies before implementing the equivalent of a social experimental laboratory.

The now-named biometric surveillance is a technology that detects, tracks, and identifies individuals of interest by their faces. FRSs make the identification and verification of users possible by comparing facial images against templates stored in databases, and have diversified into their uses and have substituted the operators of the previous manual systems. In any of these cases, the facial recognition process involves face detection and localization, face alignment, facial features extraction, and recognition. The popularity of FRSs is due to the fact that decision-making processes based on the use of FRSs are quick and easy to use. Additionally, it is configurable and can operate in open or closed loop mode. Commercial FRSs provide solutions for different applications, such as locating suspects in crowds, monitoring people at events, finding missing persons, surveilling border areas, controlling access to secure locations, surveilling public safety, carrying out identity checks, locating people with outstanding warrants, or counting and monitoring the mood of people who visit stores among many others.

12.3.2. Drone Surveillance

The integration of drone surveillance, technically known as unmanned aerial vehicle technology, into law enforcement operations has expanded significantly in recent years. The use of UAVs for policing purposes was virtually nonexistent until the early 2000s, as the technology needed to build an inexpensive drone with sufficient flight time and camera capabilities did not exist. The earliest adopters of drone technology were military agencies, and military drones generated copious and useful intelligence at minimal risk to soldiers, allowing for interventions such as changing the course of certain terrorist attacks. The military's positive experiences did much to encourage the use of drones for law enforcement purposes.

In the United States, police and the military have long shared information and technology, although perhaps to a degree unique to the United States. Indeed, the line between military and policing in the United States is tenuous at best. Law enforcement agencies, especially counter-terrorism units, began attempting to deploy small drones for specific missions in the years after 2001. In 2006, the Miami Police Department flew a drone over sporadic rioting during the annual celebrations. After a traffic collision in California resulted in a muffled explosion amid a crowd of festival attendees, law enforcement attempted to use a large drone to enhance surveillance of a music and arts festival. Policing with UAVs, however, did not take off until the last third of the first decade of the century, as UAVs were utilized to assist in locating and stopping armed suspects.

12.3.3. License Plate Recognition

License plate recognition is a comparatively simpler technology, routinely in use for many years. However, it is increasingly seen as privacy-invasive, especially in the context of automated plate reader usage. License plate recognition is accomplished through a variety of methods. The easiest method is the manual entry of the plate number, which many screeners still prefer. There are specialized databases into which such manual entries can be put, but for high-volume this approach would be very tedious. The next most efficient method is manually reviewing a photograph and making an entry into a database, which requires recognition of the characters in the license plate but is significantly easier than recognizing and entering patterless text in an arbitrary font. The next succeeding layer of automation takes the form of optical character recognition being applied to the plate number in the photograph. The highest-performance approach, of course, is OCR without human review.

There are many competing commercial and open-source solutions available to law enforcement agencies, including ALPR software developed in parallel, as well as open-source software. These software packages can be added to common platforms. For example, software can be integrated with surveillance cameras from various manufacturers. With all of these solutions the OCR process is extremely reliable, giving near 100 percent reliability with proper camera placement, good lighting, a clean plate, and so on.

12.4. Predictive Policing

Predictive policing relies on statistical forecasting to analyze historical crime data and employ it to solve new cases in law enforcement. Predictive policing solutions that fall short of real-time analytics seek to anticipate potential crimes based on insight from a

variety of past offenses. These tools help reduce dependency on patrols in hot spots in order to boost police efficiency, without threatening civil liberties and social justice. Most predictive policing solutions are spatial models that determine where crimes will happen based on historical patterns, or temporal models that forecast when a new crime will occur. Other tools aim to prepare police agencies for potential problems by evaluating factors such as the social conditions linked to homicide, the economic conditions linked to aggravated assault and property crimes, or the real-time assessment of the risk of gang killings. Some jurisdictions also rely on algorithms to forecast which specific individuals are at risk of violent crime based on analysis of criminal histories but lack the real-time capability needed to inform patrolling decisions.

Data-driven policing methods are now widespread, computerizing standard, time-worn police practices using predictive algorithms and millions of police records. In particular, over the past decade, U.S. law enforcement agencies have grown increasingly reliant on statistical prediction tools employing big data to identify crime-prone areas or individuals across the territory under their control. The anticipated explosion of sophisticated spatial-temporal predictive models able to replicate and upgrade this kind of police practice along with a remarkable public safety justification has put the issue of civil liberties across the nation on the back burner. The widespread use of data-driven predictive solutions is not, however, a policy recommendation. The potential benefits of using statistical algorithms in police investigations are accompanied by serious risks of unaccountability, lack of transparency in decision-making, and possible reinforcement of social inequalities if the outputs are not properly supervised or carefully used.

12.4.1. Data-Driven Approaches

Data-driven approaches to policing have received major attention from law enforcement agencies and other advocate organizations. In contrast to traditional policing strategies, which use the agency's discretion and officers' experience for patrol direction, these emerging methods implement machine learning algorithms trained with historical offense data to guide police agencies on where and when to intervene. These data-centric strategies can be categorized into two groups. The first group of studies produces an intervention plan. In this group of studies, the algorithm is exposed to historical events and decides the locations and the times with the highest predicted number of incidents. The second group of studies use machine learning for incident and suspect identification and risk assessment. As opposed to being purely geographic, these data-driven methods are processes implemented on people's personal data.

Both groups of studies predominantly rely on geospatial and temporal statistics. Most of the times, these two types of attributes are the only ones used by emerging predictive strategies in the first category. On the contrary, the second group of studies can

sometimes rely on demographic data, social media type information, link analysis, or larger socio-technical decision processes. These differences in approaches might seem minor. However, they can produce a stark contrast from a capability perspective on what police can predict and the type of interventions that can be enforced. In addition, two completely different privacy issues emerge from these two categories.

12.4.2. Risk Assessment Tools

Risk assessment tools, intended to estimate the probability of a suspect committing a future criminal act, have been adopted by law enforcement agencies and judicial systems. These tools usually rely on complex machine-learning models, which examine an extensive list of variables and then look for patterns that may indicate a higher risk of committing a new crime. Recently, these prediction scores have been presented to judges and used to inform their decisions. Although advocates of these types of assessments often present them as an objective method of making extremely difficult decisions, there are substantial ethical issues with risk assessment algorithms being used in this way. First of all, some people contest the validity and accuracy of the algorithms used. In fact, to the best of our knowledge, the actual algorithms have never been released by developers, and independent audits have been prevented by contractual limitations. This has led external researchers to conduct investigations into how well existing risk prediction algorithms actually perform.

Acting as an outcome predictor, a risk assessment tool could be explained and audited by inspection. If there would be a need to test its performance, this could be done using criminal statistics. Even suggesting that the results are reliable can lead to incredibly negative consequences, as demonstrated by the use of other algorithmic models. Even aside from the inherent problems in the creation of these models, risk assessment tools should not necessarily be used in such decision-making scenarios. For instance, research in psychology and law has shown that human judgment in predicting criminal behavior may be even more accurate in some scenarios than existing risk assessment tools, especially when additional informative situational cues are considered.

12.4.3. Case Studies of Predictive Policing

While many predictive policing forecasting techniques and tools are commercially available, few have been thoroughly evaluated. Research into specific examples of predictive policing models may help illuminate the strengths or weaknesses of certain methods, as well as allow viewers to better gauge the weight of any presented empirical results. We note the important difference between crime forecasting models, which utilize predictive modeling as a method of resource allocation, and forecasting-guided

resource allocation models, designed explicitly for the purpose of limiting resource allocation to high-need areas controlling resources across space and time.

In 1901, using available arrest data, the first model-based approach to crime forecasting was developed and implemented in a New York City precinct. A prediction and simulation of the effects of a simple local regression based algorithm on the concentrations of deploying officers in both space and time report a reduction in crime rates of 19% when the method is applied to a high crime area. In addition to officer allocation, crime forecasts are provided for use in deployment of police cameras. To utilize the model, police departments must obtain camera video images and forward them, which then relays forecast messages back.

The model clusters crime predicted times over the next 12 hours into ten groups, and additionally provides descriptions. Repeated interviews with seven participants indicate that crime plan developments change predictively due to the model results. The validated and peer-reviewed model internally allocates the highest predicted burglary and robbery county-rate decreases across space by day or hour. Also, the practitioners stress that the core difference is its law-enforcement custom-made nature, which differs from public-open source software.

12.5. Ethical Considerations

While these advances can translate to more effective law enforcement and increased security, they may also cross certain ethical and legal boundaries. Applying AI in law enforcement raises significant ethical debates. These involve considerations of legality in the enforcement of the law by law enforcement agencies, code enforcement, and the used technologies' overall goals. At the same time, due to the heterogeneous nature of law enforcement, it remains a misnomer that there exists a singularly defined body of ethical bylaws that pertain directly to all law enforcement action. Law enforcement is often a reflection of the larger systemic societal mores. Therefore it might be the case that more universally established philosophical frameworks can be best utilized to chart out ethical considerations of AI's application.

Ethics are usually defined relative to the concept of 'the good'. At its most general level of abstraction, 'the good' can be conceived as a standard condition that causes people to attribute satisfaction regarding the state of the world. Based on the 'good' concept, two major basic ethical frameworks that guide mankind’s behavior and help keep moral equilibrium have been devised, namely: Consequentialism, which promotes the idea that the results of actions must be carefully worked out, so that the world moves to a state in which the good is maximized; and Deontology, which states that there are certain pre-defined behaviors that are valid universally, and must always be abided by, regardless

of consequences. Furthermore, these pre-defined behaviors can be rigorously defined by means of human rights, which can be defined as a set of universal moral standards that cannot be infringed.

12.5.1. Privacy Concerns

Privacy is a central concern for the social acceptance of AI-based surveillance systems. Because such systems often infringe on the privacy rights of the citizenry, it is necessary to justify surveillance by demonstrating that it protects the right to security and that this is in a reasonable proportion to the extent of privacy infringement. Surveillance is furthermore set against the background of the existing legal framework regulating privacy rights and the permitted uses of surveillance systems by law enforcement agencies. Data protection laws categorically prohibit specific surveillance systems or uses in specific contexts. Thus, surveillance systems that disproportionately reduce citizens' privacy have to be justified within the existing legal framework. In cases where hate speech is proscribed by law, the need to protect citizens' freedoms of expression and impression can complement the need to protect citizens' privacy rights in limiting the operation of content moderation algorithms. In result, if there are functioning institutional measures in place, such as hotlines, that would allow citizens to report posts or activities that would result in a reasonable risk of causing imminent, serious harm to the public or specific individuals, then it is possible to safely operate a content moderation algorithm.

Some of the features that would have to be present to minimize privacy concerns regarding AI-based surveillance systems include informed consent by the public regarding the type of surveillance employed in specific contexts, the express purpose of the surveillance system, as well as its operating mode, i.e., active, semi-active, or passive. Concerning passive surveillance systems that monitor citizens in public spaces, not only the citizens physically present in the monitored area, but also citizens without any specific connection to an ongoing security incident be made aware of the privacy risks, both present and potential. Moreover, the purpose should to some extent align with citizens' personal interests.

12.5.2. Bias and Discrimination

Algorithms implicitly create norms of fairness that are then externally imposed in a more discriminating way. Using biased data, it can worsen the situation by reinforcing or exacerbating prejudice. AI's ability to deal with structural discrimination from databases can either take away the ethical burden from law enforcement agencies by simply showing data as is or catalyze its implementation. In cases with little or no supervised

data, exploiting AI for decision-making is extremely dangerous because of the unpredictable outcome. Bias and discrimination in law enforcement have existed long before AI and have been present in records, which in some cases still retain sensitive information about the social class, any health issues, religious beliefs, disabilities, sex, gender identity, sexual orientation, nationality, or ethnicity. The risk of discrimination and bias remains associated especially with the following populations: those who are labelled at-risk due to their specific social, economic, ethnic, or health status: migrants, homeless, the elderly, the unemployed, drug addicts, etc.; those who might be affected by violation of their civil or political rights, such as: community activists, employees of nonprofit organizations, opposition politicians, representatives of traditional and religious minorities.

Detecting and prosecuting bias in AI systems is extremely difficult, because most software tools considered biased make a decision for a short period of time in the process of a very complicated and non-obvious process involving many other phases and probabilities. Only the last part of this decision-making offers an opportunity for validation of the quality of AI-based algorithms. Biased predictions should always be treated with caution and ideally should be challenged; critically, these predictions have consequences for the individual or community.

12.5.3. Accountability and Transparency

Data-driven policing has garnered attention because of the problematic consequences produced by its outputs, which might influence the resources and funds spent on criminality suppression and its impact on communities. While the separation of the data from data usage is graphically shown in the model effectiveness requirements, it does not imply that a model should be considered just a tool without its own set of requirements. How far should model accountability and transparency extend? The obvious answer is that model requirements should reflect potential impacts: the closer the decision is to a life-altering action, the stricter the requirements for that model.

If an agency is going to act on the basis of predictions, or forewarn a specific event, they would be required to most probably meet the highest ethical standards. Reality shows that criminal codes rely primarily on past action; previous patterns are normally the foundation for any punitive action. Without downplaying the importance of the predictive process, the risk of denial of due process is intrinsically linked to the application. Elimination of data from the model is ineffective in this case. The incapacity of a model to identify a biased link in data does not absolve the agency from its own responsibility of due process.

Modeling is a two-step procedure. It is understood that data opens the possibilities for massive, general, “unexplained” forecasts affecting large sectors of the general public. However, the impact of these actions must also be reconsidered: should these models exist at all? Should these kinds of predictions influence agency actions? The corrective idea is that these steps attract different types of ethical requirements, but they are not in a separate realm: accountability, transparency, and bias infiltration into the model are directly linked to its outcomes. The goal of any model is to understand some behavior according to some indicators even when these actions are not going to be specifically used.

12.6. Legal Framework

While there are pending updates due to the rapid development of AI technologies, there are existing national laws and legal frameworks that support the legislation of AI use in Law Enforcement. Such frameworks and legal processes address common issues regarding ethics and accountability concerns surrounding the use of AI; hence, they can be successful in regulating the use of AI technologies. Also, if AI is introduced in a manner that causes a legal dilemma in regards to existing laws, these legislations themselves can be updated to address present and future dilemmas of law enforcement responsibilities. The lack of regulative frameworks referring to the use of AI technologies in Law Enforcement is essentially observed in a handful of countries. For example, Canada is among the few countries that implemented a moral and ethical guiding document that can assist police agencies in making ethical, socially-acceptable use of AI technologies. Other countries have visible frameworks and drafts that could assist states in making legislative or regulatory decisions around the use of AI. More precisely, a draft was released which builds on guidelines and recommendations stating that such guiding documents can regulate the use of AI technologies present in law enforcement processes. However, countries with concerns regarding the use of guiding regulatory documents can use existing general laws related to technology, security, and ethical principles of respective countries to assist regulating AI use in Government processes, including Law Enforcement.

12.6.1. Existing Laws and Regulations

The existing legal framework regulating the use of AI in law enforcement is shifting and largely inadequate in the United States and internationally. Deepfakes, for example, have upended traditional concepts of truth in media and the jurisprudence regarding freedom of speech, and need targeted laws against specific malicious uses. Current laws regulating online freedom of speech either don't apply to deepfakes because the creator

is not claiming credit for their work, or provide for little relief in competition contexts because they only allow recovery of actual damages. Facial recognition software has, over the objections of tech experts, become an indispensable tool for law enforcement investigations. Laws protecting against its misuse are possible, proposed, and pending both on federal and state levels, as is currently being discussed.

A spokesperson reminded reporters in response to a question about privacy concerns and law enforcement use of VR and other technologies that, "Law enforcement works for the people. If people are concerned about a police agency's use of the technology, they should reach out to their local officials." Ending an unwarranted blanket surveillance and tracking of its citizens is a primary motivator of many of the currently proposed state and local restrictions. Although a common response to an increase in technology surveillance is mandated transparency, such requirements are generally weak and often ineffective. A primary proposal to increase the efficacy of disclosure laws is to create specialized sources that aggregate available information in a meaningful way for the public. However, this does not address the need to provide disclosure for basic connection technologies like cell phone tracking, real-time monitoring of cameras in citizens' homes, and agency use of private cameras and data, particularly in sensitive areas such as near houses of worship and voting places.

12.6.2. Proposed Legislative Changes

While the president's executive order requires urgent attention and requires much more text as it is too general, the following legislative frameworks represent more detail in regards to what should be banned and how.

For example, it is wise to more carefully define the circumstances regarding the necessity of the implementation of AI surveillance systems and declare violations of existing legislative frameworks. However, currently gaps exist that allow for wrongful surveillance to occur. Consequently, it is proposed to add the following laws within the context of a legislative framework:

The intent of this framework is to limit surveillance so that it is required for safety laws or security features. Indeed, entities require permission to perform surveillance, especially at risk or vulnerable populations. On the other hand, while addressing privacy concerns in recent drafts of legislation that would apply to commercial entities perceived socially as intending to surveil, for now nevertheless remains focused on the corporate sector and the design of associated oversight and governance structures.

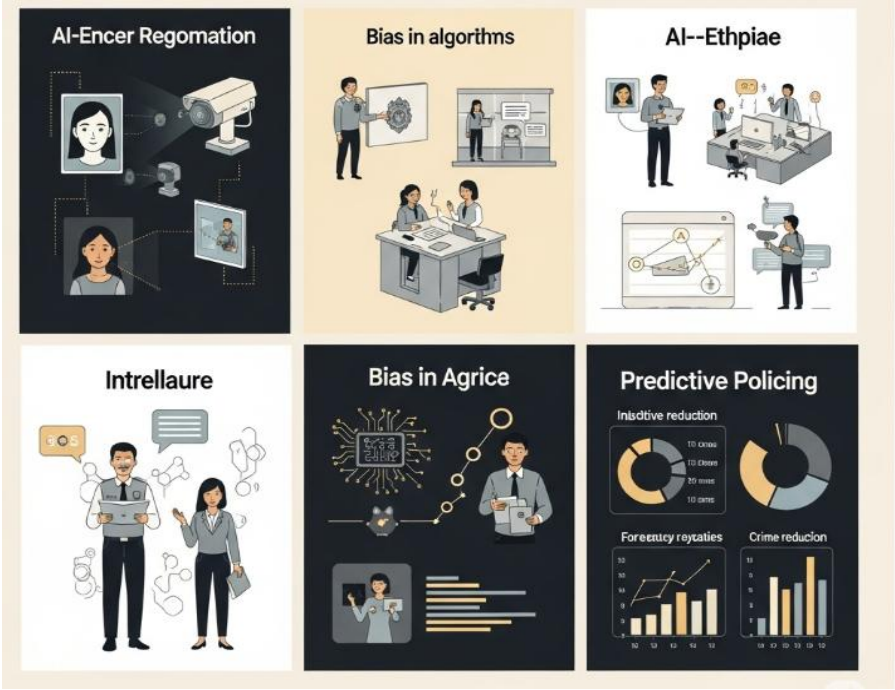

Fig 12.2: Predictive Policing using Machine Learning

12.7. Public Perception of AI in Law Enforcement

The technology adoption process has an additional phase in law enforcement outside the business environment, which is not present in adoption models: the social acceptance of the technology. Citizens have a different opinion than law enforcement agencies about the use of AI in policing. If the majority of Policing 2.0 is about tourists inviting algorithms to oversee their experience, an unequal discussion will produce consequences in the inter-twin observatory-expected agency during the operations in Policing 2.0 matrix. Cultural products – from films to news – considering the surveillance technology are key elements to detect the context of possible dilemmas about the use and scope of algorithms in Policing 2.0.

The news narrative about police algorithms is often negative. An increasing number of research papers detect that balance and that agents discuss not showing an interested neutrality. At the same time, many surveys reveal that people consider surprising news when listening to them denouncing the possible errors of algorithms, especially about a social issue that citizens consider very important: the fear of the use of AI in law enforcement stating it will not be an observable element. The first point is that, in a rush, citizens support AI in policing, in a second phase, the concern about the consequences of algorithms for citizens' rights accompany this use.

12.7.1. Surveys and Studies

Public support for surveillance technology in law enforcement varies from positive to negative stances, and newer forms of surveillance face more pushback than older technologies. Positively reviewed are technologies that seem to augment law enforcement capabilities, while in contrast, negatively reviewed are technologies perceived to reduce privacy. For example, cameras monitored by either a third party on behalf of police or police themselves capture significant public support, though this support diminishes significantly in the case of facial recognition used by police.

The survey results appear to show that public opinions about police adoption of surveillance technologies are often skeptical. Public trust in law enforcement institutions may be highly conditional, contingent on the specific technology in question, and, thus distant from actual use conditions. The novelty of the technology itself is not sufficient to generate strong negative emotions; on the contrary, the technical novelty can trigger curious adoption and positive appreciation. It is not a simple task for law enforcement agencies or other actors to predict public acceptance of the newest appeared technological tools. A very narrow trust gap could form between police and communities when agencies promote implementation of newer technological tools without sufficient and clear explanations.

People in general find AI-enabled prediction policing less acceptable than traditional police actions such as checks or stops. Widespread negative feelings toward AI-enabled prediction policing seem to derive from AI's perceived ineffectiveness, reflecting possible flawed sensing and deciphering activities. Furthermore, a general skepticism of law enforcement effectiveness might also be a potential reason for the negative public sentiment regarding AI-enabled prediction policing, especially for communities that are already suffering from the negative effects of community-level crime. AI-enabled prediction policing is considered acceptable only for cases with high levels of susceptibility and high levels of police-facilitated rumor control.

12.7.2. Media Representation

The majority of research into public perception analyzes survey results; however, public reaction is also portrayed in the media. In this way, the media shapes social norms and can even shape a community's risk perception. Portrayals in the media can be a mundane reporting of facts, or can take the form of editorializing and opining by choosing what stories to cover and how to present them. Research has shown that both fear-inducing television reports and direct experience can influence public perception, increasing or decreasing the demand for security measures and condoning or opposing their use. The media impact ranges from reflecting public opinion to agendas and attitudes that drive

policy decisions, often in conflict with empirical observation. Research also highlights the connection between the media and the entertainment industry, specifically concerning movies. The popularity of a particular genre and the specific topics covered can drive interest, both positively and negatively, in the particular industry.

We analyze a sample of existing media coverage, exposing our analysis of current public perception. We found that, similar to other analyses, English-speaking sources feature overwhelming positive coverage while other languages feature more neutral to negative stories. Since this difference is one of quantity, it could influence public perception through the sheer amount of articles people might be exposed to, coupled with the fact that most people will trust what they read in their own language. Moreover, we note the impact positive representations of AI will also affect future development, and drive customer support but will only create active demand for these tools as the number of depicted scenes of being protected or helped outnumber negative emotions, drawing ideas from the manipulation of reverse trends via the use of co-occurrence word trees.

12.8. International Perspectives

While AI is rapidly being integrated into law enforcement globally, widespread adoption is still limited. Many of the pioneering AI law enforcement projects have been carried out in Israel, where the high level of threat posed to the nation by the neighboring territories and other opponents has driven many national policing agencies to push the envelope regarding law enforcement technology. Forecasts predict AI law enforcement spending to increase significantly in the coming years, as interest from law enforcement stakeholders grows and access to technology continues to democratize.

In Israel, law enforcement decisionmaking is heavily reliant on national security intelligence gathered by various internal and external security agencies. AI capabilities have been developed to serve the needs of these agencies, often using investments from both national security and law enforcement funding streams. The law enforcement agencies include the national police and border police, the ministry of public security, the internal security agency, the ministry of homeland security, and the ministry of transport security. During the last few years, Israel has seen various initiatives to develop its police capabilities in the AI domain. Five special focus areas were emphasized in the plan: Investigation – AI technologies will augment the investigative capabilities of police detectives.

The use of AI for law enforcement is likely going to be uneven. In liberal democracies, there is considerable public concern over the use of facial recognition and other technology-based solutions, which could lead to a backlash with respect to its societal acceptance. In authoritarian-controlled states, the law enforcement apparatus tends to

favor the use of these AI tools with little to no opposition, which could lead to widespread societal monitoring and control.

12.8.1. AI in Law Enforcement Globally

AI's influence is especially visible in the police areas of security and surveillance. Many police forces increasingly rely on drone technology to monitor neighborhoods and streets, probably in parallel to the increasing use of drones to curtail protests and civil unrest. Such enhanced surveillance possibilities are combined with AI tools, like facial recognition, real-time online mapping, predictive policing applications, license plate recognition, and predictive gunshot smoke detection. AI classification in these fields of law enforcement is useful to speed up the identification and categorization of data, to police future events, such as crime, civil disturbances, or even terroristic attacks and optimize deployments.

However, the increasing use of algorithmic tools to boost efficiency in the law enforcement process, especially of prediction tools, can place existing and additional burdens on individual freedom and rights, as well as encourage discrimination, profiling, or stereotyping behavior on the part of law enforcement personnel, particularly in regard to people from diverse ethnic and cultural backgrounds or involved in precarious economic situations. Therefore, these new tools may raise questions regarding accountability for mistakes made both by the AIs themselves, or by the authorities relying on the outputs of those AIs. These aspects will most likely be at the heart of public and political discussions in the relevant countries about the increasing role of AIs in the field of law enforcement. The following cases illustrate the current practice and concerns regarding the future of AI tools in law enforcement in some selected countries.

12.8.2. Comparative Analysis of Different Countries

In the preceding section of this chapter, we noted and elaborated on the fact that currently there are many nations and territories globally that are applying AI in wide-ranging aspects of policing and criminal justice administration. In this section, we provide a comparative analysis emphasizing and discussing applicable examples from various nations and jurisdictions in an effort to identify some of the many variations in AI applications being employed and experimented upon globally in the realm of law enforcement.

While academics and practitioners based in one nation are driving the development of popular AI visions and algorithms utilized for Smart Policing, another nation's police are at the forefront of using AI-based decision support systems to help fend off potential

future threats to social stability. These tensions, revealed as riots and protests storm through both nations, are exacerbated by the rising influence of the diaspora and migrants on either side. The police forces thus use various Artificial Intelligence-based Predictive Policing systems that take cues from social media, identifying incendiary content on internet platforms, identifying hate speeches, and posting call-to-action clips to target inhibitors. During the course of unrest, many AI tools are deployed to surveil the offenders and assist the investigations. Further during the law and order procedures, police often deploy AI tools to develop facial recognition and video analytics systems that help identify rioters and offenders engaging in unlawful activities, development and maintenance of Machine Learning-powered Intelligence Systems designed to predict unlawful activities during a riot or unrest, and AI tools to map social media networks. During the pandemic, police turned to AI with a vengeance to develop and maintain Facial Recognition and Video Analytics Systems programmed to detect and identify mask violations of the citizens out there on the streets.

12.9. Challenges and Limitations

Law enforcement agencies are increasingly turning to AI-assisted techniques to help improve their operational effectiveness and address resource limitations. However, AI approaches are not a panacea. There are significant technical and operational challenges limiting the use of AI-based methods in policing and other law enforcement domains. Furthermore, AI has the potential to exacerbate already existing public distrust issues related to policing.

The application of AI technologies to law enforcement tasks is in its infancy, and most implementations are experimental prototypes without sufficient initial validation or testing on key evaluation metrics. Many of the law enforcement applications of AI are still reliant on classical data mining techniques, such as prediction-based modeling, and incorporating more advanced AI-based techniques raises challenges. For example, the police have access to a vast number of datasets with associated annotations. However, many of these datasets are not properly labeled or are stored in different databases and require extensive cleaning and preprocessing before they are suitable for AI training. Even when labeled datasets are available, they are typically not large, which raises issues related to generalizability and overfitting. In addition, the data collected are often noisy, inaccurate, and subject to biases based on historic policing practices. These issues may be significant for a variety of tasks, including facial recognition and video analytics. Furthermore, many of the AI approaches developed for specific tasks rely on supervised learning, which may require extensive fieldwork to label and annotate training images.

As law enforcement organizations worldwide continue to undergo extensive scrutiny focused on systemic community bias and mistrust, the introduction of AI paradigms may

be met with significant resistance from the same communities that have been negatively affected in the past. These sentiments are further amplified by the fact that AI-based systems, particularly those based on statistical learning and similarity matching, may not take into consideration the history or context of people exhibiting certain behaviors and can misinterpret them.

12.9.1. Technical Limitations

There are significant differences between how facial recognition systems work and how human beings recognize faces that illustrate the challenges of computer vision. The most important of these is that FR technology is fundamentally different from human recognition of faces and does not utilize the same mechanisms. Humans have specialized areas of the brain that are highly trained for the task, while FR technology is not using such specially developed mechanisms. Although highly developed, FR technology is sensitive to changes and can operate poorly under a variety of conditions that are not problematic for human recognition. For instance, recognition at a distance or in adverse lighting conditions can be significant problems for many face recognition systems today and loss of resolution due to distance effects, where the face in the image being analyzed has whom the lose of individuals at a distance can cause problems for human observers as well. Recognizing faces that are dirty or partially occluded is much more problematic for FR systems than for humans. Humans can recognize a person by their whole face, or by just memorizing a portion of a face whether it be the eyes, nose, or some other aspect of the face.

FR technology also requires a variety of other conditions that are less important for human recognition. FR relies on high-quality images, preferably taken in good lighting, where the person is facing the camera with their features clearly visible. Differences between what would normally be considered a “normal” image for human recognition and what is necessary for FR technology have led to discontent with the technology. For example, inter-ethnic variation in the appearance of human faces can be much larger than intra-ethnic variation, where people have been egregious failures in recent years, with the AI unable to accurately recognize women of color. Consequently, a recent growing mania about AI is that, outside of the potential release of large models in the future, it is likely that such facial recognition systems, especially no-parameter systems, will be deeply unsatisfying to the general population, especially, say, young people of color, or other marginalized ethnic groups that can obviously be impacted by this technology.

12.9.2. Operational Challenges

AI systems require extensive data sets to generate accurate actionable results, but every new application needs a data set unique to the circumstances of its deployment. For example, during the height of the pandemic, researchers used a large number of Tweets to train officer-facing software to detect when people were not social distancing and the risk they posed. Additionally, officer and supervisor input is required for machine learning AI to effectively monitor surveillance camera feeds. Just as with AI-generated facial recognition, input from law enforcement is essential to identify characteristics unique to a specific incident or area, such as time of day or background objects. Additionally, understanding how potential criminals may exploit these factors to avoid detection is crucial to maintaining a functional system. Other datasets, mostly in the form of metadata, would be needed for AI systems facing the public.

Even with these unique data sets, accurately recreating the results of these simulations is impossible. Significant tradeoffs exist between accuracy and false positive rate, and achieving reasonable precision on a complex problem generally requires a custom-designed expert system. Because almost every implementation of machine learning in the public sector uses an off-the-shelf solution, little to no official analysis exists on the level of public sector administrative support that would be needed to attain reasonable accuracy. Since most government AI applications are built without official collaboration with vendors, the results of prior implementations are likely not accruing to the public sector.

Convoluted and multistage administrative processes are common throughout law enforcement. These processes can easily add unnecessary delays to the analysis of incidents by violating private vendor best practices or budget and contract guidelines. Additionally, some stakeholders may first become involved in incidents through the release of sourced materials, inhibiting internal analysts from using sensitive results first. The existence of these severe limitations raises serious questions about the actual utility of data pooling, as suggested by various scholars.

12.9.3. Public Trust Issues

The collection of citizens' personal data has been a common practice of both public and private institutions for many years, in an effort to build comprehensive profiles that could be useful for various reasons. These data are often used for purposes other than those for which they were originally collected or even sold to third parties. The metadata resulting from data collection are, however, incomplete: they can only show patterns of behavior based on pre-established characteristics, but they cannot explain the reasons for the choices and behaviors inherent in individuals. In this context, the availability of

resources of Artificial Intelligence allows for augmented decisions, but it is important to remember that certain possibilities may exist that the decision maker will rule out. For example, the police may decide to stop surveillance of a particular neighborhood where it discovered a pattern of recurrent crime leaving the inhabitants of that neighborhood outside the number of profiles that are usually considered. These decision makers cannot ignore the reactions of the users who are being observed for a longer or shorter time: public institutions are called to defend the public good and there could be serious negative repercussions for a community subjected to massive surveillance without the threat of an immanent criminal act.

The inadequate protection granted to citizens from violations that lead to erosion of their personal freedom and damage to their image or violation of their privacy can create deep-rooted distrust towards law enforcement agencies and questioning on their actual role and mission, if their only purpose is to ensure security through methods that openly violate citizens' fundamental rights. The observation of sensitive communities is likely to lead to the identification of a type of "criminal" regarded as linked to that particular environment, which in turn would worsen or install a state of tension that could only discourage those who are members of that community in reporting crimes, precisely when a police presence in an area would serve to stimulate citizens to speak out. The use of AI in operations carried out by entities mandated to ensure public safety could thus trigger a perverse feedback process: data collection would not bring about the hoped-for results but would fuel distrust towards law enforcement agencies that, in extreme cases, would only be considered as a permanent threat.

12.10. Future Directions in AI and Law Enforcement

The future of AI technology in American law enforcement poses both risks and opportunities for agencies and officers. On the one hand, improvements to existing tools, combined with wider policy applications of AI from partners in other real-world sectors, hold the promise of advanced but practical solutions to the problems of police and policing. On the other hand, new but local adoption of unfamiliar AI tools without clear policy restrictions but with a lack of institutional public safety experience could squander institutional resources and damage public trust. Finding a common ground where effective AI law enforcement tools are used prudently with the shared institutional experience of local, state, and federal agencies would maximize the opportunities and minimize the risks of AI law enforcement technology.

Various agencies have reiterated their commitment to working with industry partners to create trusted AI technology. Through research and policy recommendations regarding trustworthy AI technology, the partnering agencies can help avoid pitfalls of untrustworthy technology while advancing real-world applications of technology. There

are many areas of research at the intersection of AI and law enforcement in which such funding would be well invested. Areas like AI-assisted crime analysis, AI-powered decision-assist systems, and systems for detecting cyberattacks would serve law enforcement agencies well. With proper research and funding, trusted AI tools would mitigate the higher cost of using untrusted tools. Additionally, the risk of public pushback against the funding would be minimized, as the tools would be at the service, not the cost, of the public.

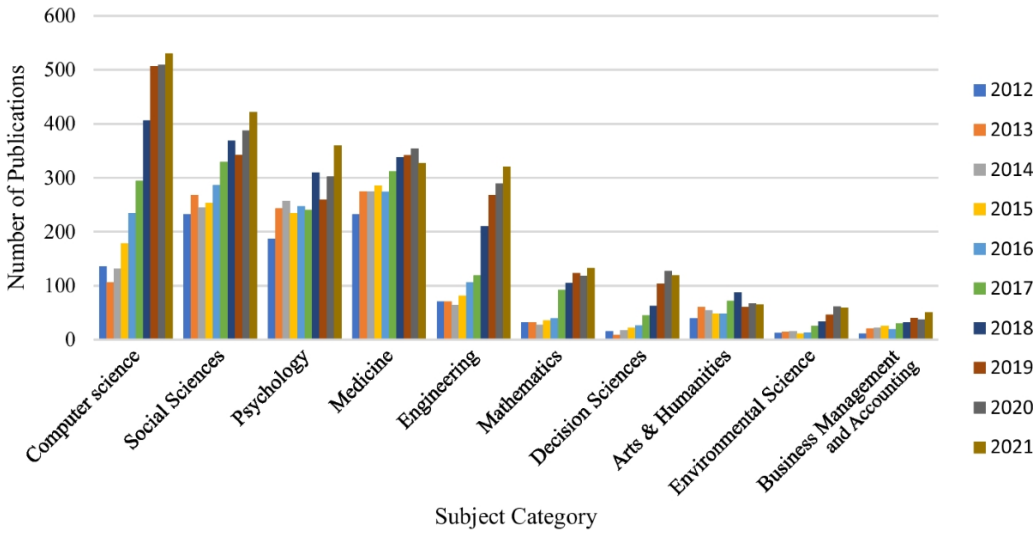

Fig : Role of Artificial Intelligence in the crime prediction

12.10.1. Technological Advancements

As discussed, increasing surveillance capabilities and proliferation of digital media offer law enforcement invaluable insights into national and community policing efforts. A principle from AI 101 nowadays seems pointless: more data means better models. Camera resolutions increase, privacy barriers fall, and the data deluge gathers scale and speed. Our concerted efforts to collect digital trailheads are matched by the increasing capabilities of AIs to help us sift through both sides of this data river to recognize patterns, build lifelike models, and guess what we all might do next.

But the current and near-term offering are already humbling: what might be beyond our imagining? What unbelievable capabilities might liaisons between law enforcement, big companies who move fast and break things, and research universities with decade-long employment commitments be able to bring to the service of national and community security? Cameras with zoom ratios no longer limited by physics (or at least, movie-like

handheld devices that can see what a surveillance plane could see?) AIs capable of producing historically accurate or photo-realistic replays of violent offenses, to be used to track and lead investigators down the path of successful prosecution? Both tomorrow's social media and AI doodle artists provide clues about latent motives. New kinds of AI agents studying the crowd-specks of a hundred-dimensional representation of traffic on the measuring bridges of the Bay Area could reinforce alarms put forth by existing models trained on rolling swathes of historic data.

12.10.2. Policy Recommendations

In this essay, we did not explore the wide and diverse range of policy recommendations that has emerged around AI in law enforcement. Given the converging characteristics of France, Germany and the UK, we narrated our accounts of the vague legal landscape and the ghostly presence of alternative policies, each with their issues of feasibility and zapotage that, in a way, is not very different from standard security guidelines.

So what can law enforcement authorities do? There are many developing strategies on what policies can and cannot stimulate collaborative, privacy-sensitive technological development. We do not pretend to list all the possible stakeholders who may be interested in reading these lines. We want to inspire the type of thinking that enables policymakers to be pushy without being too noisy.

While funding teams concerned with the impact of proposed technologies on the lives of those affected by decisions being buffed may help, a more virtuous approach seems to lie in the avoidance of creating a reliance on insider knowledge about what technology can do. Then it is time to rethink the operational ceiling for infrastructures such as the GSC and DGSI OPCAT. While minimum policy guarantees may limit any possible capacity for testing legislation-based AI applications, we suggest such policies be implemented through intervention methods with specific and transparent exit strategies.

A second avenue relies on collaboration's exchange nature motivating joint effort for better return on investment in society. To make collaboration attractive, transparency in commitment is clearly needed; the various steps that regulators will adopt in the event of non-compliance on the part of the industry must be explicit and communicated in advance.

12.11. Conclusion

The use of AI, if left unchecked, could lead to infringements of civil rights. Police agencies should not only comply with laws but also be ethical. When using AI in law

enforcement, it is important to focus on accountability, public participation, and clarity. Law enforcement's performance, productivity and output impact society. While mistakes can be made, law enforcement bears a bigger burden, as an error could adversely affect citizens' lives. While public safety is paramount, police agencies should refrain from excessive use of AI technologies, and instead work toward building community trust and partnership. Public safety and policing are not the same, with the latter being one of the components used to ensure public safety.

All AI products being used in law enforcement should be accurate and transparent. Police agencies should conduct real-time surveillance to mitigate risks to those toward whom AI products would be deployed. The industry should acknowledge and address brown, black, and diverse communities, as they are continuously under pressure of having products that do not benefit them, yet could harm them. Everyone should have an equal opportunity to enjoy the benefits of AI technologies, as this balance is of great importance. Also, the laws should be clear in terms of stakeholders' rights. If something goes wrong during the process of deploying technology, it should be clear which party is responsible. Technologies used in law enforcement should have complex control in terms of policy, with technologies meant for sensitive applications requiring tier-one pathologies prior to launch. Law enforcement is a people business, and it should be concerned about the lives of the people who police their communities. Police agencies should focus on trust, as it is the cornerstone of every successful partnership, and a great opportunity would be lost if these products replace positive engagement with communities.

References

Ferguson, A. G. (2017). The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. NYU Press.

Brayne, S. (2020). Predict and Surveil: Data, Discretion, and the Future of Policing. Oxford University Press.

Joh, E. E. (2016). “The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing.” Harvard Law & Policy Review, 10, 15–42.

Garvie, C., Bedoya, A., & Frankle, J. (2016). The Perpetual Line-Up: Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy & Technology.

Lum, K., & Isaac, W. (2016). “To Predict and Serve?” Significance, 13(5), 14–19.