

A Systematic Review of Using Machine Learning and Natural Language Processing in Smart Policing

Paria Sarzaeim ^{1,*} , Qusay H. Mahmoud ¹ , Akramul Azim ¹, Gary Bauer ² and Ian Bowles ²

¹ Department of Electrical, Computer, and Software Engineering, Ontario Tech University, Oshawa, ON L1G 0C5, Canada; qusay.mahmoud@ontariotechu.ca (Q.H.M.); akramul.azim@ontariotechu.ca (A.A.)

² Mobile Innovations Corporation, 5833 Marshall Road, Niagara Falls, ON L2G 0M5, Canada; gary.bauer@mobinnoco.com (G.B.); ian.bowles@mobinnoco.com (I.B.)

* Correspondence: paria.sarzaeim@ontariotechu.net

Abstract: Smart policing refers to the use of advanced technologies such as artificial intelligence to enhance policing activities in terms of crime prevention or crime reduction. Artificial intelligence tools, including machine learning and natural language processing, have widespread applications across various fields, such as healthcare, business, and law enforcement. By means of these technologies, smart policing enables organizations to efficiently process and analyze large volumes of data. Some examples of smart policing applications are fingerprint detection, DNA matching, CCTV surveillance, and crime prediction. While artificial intelligence offers the potential to reduce human errors and biases, it is still essential to acknowledge that the algorithms reflect the data on which they are trained, which are inherently collected by human inputs. Considering the critical role of the police in ensuring public safety, the adoption of these algorithms demands careful and thoughtful implementation. This paper presents a systematic literature review focused on exploring the machine learning techniques employed by law enforcement agencies. It aims to shed light on the benefits and limitations of utilizing these techniques in smart policing and provide insights into the effectiveness and challenges associated with the integration of machine learning in law enforcement practices.

Keywords: smart policing; machine learning; natural language processing; artificial intelligence; law enforcement



Citation: Sarzaeim, P.; Mahmoud, Q.H.; Azim, A.; Bauer, G.; Bowles, I. A Systematic Review of Using Machine Learning and Natural Language Processing in Smart Policing. *Computers* **2023**, *12*, 255. <https://doi.org/10.3390/computers12120255>

Academic Editor: Kartik B. Ariyur

Received: 2 October 2023

Revised: 17 November 2023

Accepted: 2 December 2023

Published: 7 December 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Artificial intelligence (AI) is becoming increasingly popular for tackling tasks that can be time-consuming for humans. Machine learning (ML) algorithms act as the key technology enabler in many fields, such as healthcare, business, law enforcement, and policing [1]. Police agencies, crime labs, and courts employ algorithms for various purposes, including administrative tools, facial recognition programs, surveillance cameras, DNA matching, and bail and sentencing [2]. These technologies are expected to achieve quicker results while minimizing human prejudices. However, they still have the potential to reflect human biases, because training an ML algorithm involves learning patterns in labeled training data, typically generated by humans [3].

In recent years, due to the increasing number of reported criminal incidents, accompanied by the growing amount of crime data, which are difficult for humans to process manually, the use of tools provided by smart policing has become more common. Additionally, the main priority of police departments is to prevent crime so as to increase cities' safety. As a result, predictive policing has been introduced as a research field, which involves a range of technologies, such as crime documentation, predictive crime maps, advanced computer software, and artificial intelligence algorithms. These tools enable the police to utilize predictive analytics, making forecasts regarding the probable occurrence of future crimes and identifying potential perpetrators and victims. The underlying rationale

behind these predictions lies in the assumption that criminal behavior and crime patterns can be predicted by drawing on criminological research and theories like rational choice and deterrence theories, routine activities theory, and broken windows theory [4].

The main contribution of this paper is providing a systematic literature review (SLR) [5] of various AI frameworks based on ML and natural language processing (NLP) that have been proposed and used in smart policing, while bringing transparency to their methods, especially those with statistical reliability to generate consistent data over multiple uses of a model or algorithm. The objective of a systematic review is to collect and provide a summary of studies that address a formulated research question [5].

There are surveys in the literature that cover different topics on ML and NLP in smart policing. One survey explored 15 studies to evaluate the possibilities of leveraging massive data repositories to scrutinize crime incidents and their correlation with different socioeconomic factors. This study suggests developing efficient computational models for crime prediction by identifying outliers, categorizing crime patterns, and employing advanced data mining and machine learning techniques [6].

Another paper presents an evaluation of several relational extraction systems based on NLP techniques according to their effectiveness in identifying semantic relations within criminal police reports, encompassing both English and Portuguese documents. The study provides valuable guidance for further research and the design of relational extraction systems for relevant domains [7].

One review paper presents a comprehensive and in-depth analysis of data mining applications in the context of crime by examining over one hundred applications. These applications are systematically listed in chronological order, providing a historical perspective of the evolution of data mining in crime analysis. With the growing applications of data mining techniques and the emergence of big data, the paper also addresses the need for increased training and investment in educating and empowering the youth with knowledge of the advantages, developments, and practical uses of data mining techniques [8].

Another systematic review analyzed over 150 studies, investigating the application of machine learning and deep learning algorithms in crime prediction. The study provides trends and factors associated with criminal activities by examining the algorithms and datasets used in crime prediction research [9].

As there is a lack of a holistic understanding of the financial cybercrime ecosystem, a survey tried to address this gap by studying the financial cybercrime ecosystem based on four factors: different fraud methods adopted by criminals; relevant systems, algorithms, drawbacks, constraints, and metrics used to combat each fraud type; the relevant personas and stakeholders involved; and open and emerging problems in the financial cybercrime domain [10].

One paper also conducted an extensive investigation into different approaches employed globally for crime prediction. The methods were systematically categorized, and their effectiveness was assessed based on precision and accuracy [11].

The present study aims to comprehensively explore the research papers within the field of crime prediction, encompassing the utilization of both ML and NLP techniques in this domain. Additionally, it seeks to shed light on the ethical challenges associated with the deployment of these methodologies. It is noteworthy that our study was carried out as a part of a research project for Mobile Innovations Corporation, which offers an application designed to empower police officers to write incident reports more quickly.

The remainder of this paper is organized as follows: Section 2 summarizes the relevant background, terminologies, and definitions necessary to understand the paper. Section 3 provides details on the method used to conduct the systematic literature review, including the research questions, and the search process used to identify the primary studies. Section 4 presents the findings and results, which consist of the list of primary studies found and the answers to the research questions. This section also presents a detailed discussion of the limitations of existing methods and the ethical challenges. Section 5 discusses a use case of large language models in the smart policing application provided by Mobile

Innovations Corporation, and Section 6 provides directions for future research. Finally, Section 7 concludes the paper.

2. Background

The rise in crime rates and the challenges that they present have sparked a need for effective crime forecasting and preventive measures. Smart policing has rapidly emerged as a response to the pressing need for innovative solutions in law enforcement, particularly in light of various high-profile cases of police misconduct and growing public demands for reform [12]. Due to the growing amount of crime data, law enforcement agencies and police departments consider the use of advanced technologies such as smart policing to process this large volume of data, offering promising avenues for crime prediction, prevention, and improved efficiency [13].

In general, smart policing refers to the application of data, analytics, and innovative technologies, such as AI and big data, to enhance law enforcement activities and ensure public safety [12,14]. It involves the development of various technologies for predicting and preventing crimes, leveraging accumulated security data and AI. Data analysis and pattern recognition play a crucial role in identifying emerging patterns and trends in criminal activities, enabling authorities to take proactive actions [15]. Additionally, smart policing tools can produce results in less time while mitigating human prejudices. Studies show that law enforcement and police departments use ML and NLP techniques for multiple tasks, such as administrative tasks, forensics, analyzing crime statistics, creating crime maps, CCTV surveillance, license plate recognition, facial recognition, speech-to-text reporting, and crime documentation [13,16].

There are also different types of tools adopted by police departments for analyzing crime data and predictive policing, which refers to technologies that use ML algorithms and statistical analysis methods to predict criminal activities and their location, date and time, type of crime, and victims of future crimes based on both historical and real-time crime data [17]. These predictions can assist law enforcement agencies in making decisions more efficiently, particularly regarding resource deployment. In theory, predictive policing is based on the assumption that crimes do not happen randomly; instead, they are followed by local environmental situations and the situational decision-making of victims [4,18]. Therefore, these technologies will help find crime patterns and aid in police intervention and prevention.

Unlike traditional policing methods that primarily rely on criminal data, predictive policing considers a broader range of data sources. These technologies use data mining methods to collect and analyze a wide range of data, including structured and unstructured data. The employed methods help law enforcers to identify crime trends, and they facilitate resource deployment and decision-making.

The shift toward predictive policing happened in the late 2000s. Before this change, a form of smart policing known as statistically informed policing, which includes intelligence-led or data-driven policing, emerged in the 1990s when Jack Maple, a New York City transit police officer, developed a crime mapping system by visualizing the locations where crimes happened repeatedly. The New York City Police Department later adopted this system. This approach, called CompStat, is now widely used by police departments worldwide [19]. It helps identify and analyze crime patterns and hotspots, measure and incentivize police activity, and allocate police resources effectively; therefore, it plays the role of a crime control and prevention method as well [20].

With the deployment of such analytical platforms, classical public statistics could now be replaced by algorithmic practices that focus on prediction by identifying clusters and patterns [21]. In recent years, the rise of algorithms has led to increased interest in studying algorithms in the social sciences. As a result, accountability, transparency, and audit have become crucial aspects of public debates about algorithms [22].

Predictive policing can also be viewed as a form of preemptive policing based on statistical data. This implies that law enforcement can collaborate with various societal actors to address the main factors that lead to criminal behavior and promote shared safety.

3. Methodology

Following the guidelines suggested by [23] and the PRISMA method [5], this systematic review adheres to a structured approach. This section elaborates on the methodology employed to carry out the literature review, encompassing various intricate procedures. It comprehensively outlines the completion of each stage of the process.

3.1. Research Questions

This study aims to answer the following research questions (RQs):

- RQ1: What methods in ML and NLP have been proposed to process crime data and predictive policing?
- RQ2: What are the strengths and limitations of the current proposed methods, and how can they be addressed?

Addressing these issues helps to gain a deeper comprehension of the present shortcomings within the field, which will lead to investigating potential solutions for the limitations of current predictive policing algorithms and devising approaches to handle text data more effectively.

3.2. Research Process

The purpose of this study was to find published papers related to the applications of AI used in policing, how it can be helpful for predictive policing, its challenges, and the proposed solutions to address them.

Following the PRISMA method, we performed our search on IEEE and Google Search, which indexes a wide range of scholarly publications, in the “incognito mode” of Google Chrome to prevent any interference from cookies. We used the following string in search engines to find the related studies:

“Artificial intelligence” OR “Machine Learning” OR “Natural language processing” OR “Deep Learning”) AND (“Policing” OR “Law enforcement” OR “Predictive policing”)

Publications written in English from journals or conference proceedings were selected, and the last search was conducted on 25 July 2023. Google Scholar offered about 25,000 results, and the first 30 pages were evaluated to identify the most relevant literature. The selection of primary studies involved reviewing the titles, keywords, and abstracts, in addition to briefly scanning the main contents of the papers to gain insights into the conceptualization of using AI in smart policing and predictive policing, its benefits, and potential drawbacks and challenges. To ensure an unbiased selection of primary studies, a set of inclusion criteria were defined. Primary studies had to fulfill at least one of the following inclusion criteria (ICs):

- IC1: Provides/lists the ML methods or frameworks used in smart policing;
- IC2: States the challenges of using AI in smart policing and how to address them.

Finally, 45 papers, including 12 papers from IEEE, were considered as primary studies. To make sure that we covered the most relevant related works, we also used the snowballing technique to find additional related works by examining the references of the primary studies [24]. Using this technique, we added 58 papers to our review; therefore, 103 papers were reviewed in total.

4. Findings

The results and findings presented in this section respond to the proposed research questions. The used algorithms and proposed tools in smart policing are identified, and the limitations and benefits of these methods are presented in this section.

Through the search process, 46 primary studies were identified, in addition to 33 papers that were added during the snowballing. In the following text, these studies serve as the basis to answer the proposed research questions in this systematic literature review.

4.1. Addressing RQ1

In general, crime can be associated with individuals or places, leading to the categorization of smart policing technologies into two main groups: One category involves location-based approaches that predict where and when a crime is likely to be committed, with a focus on relevant factors of criminal activities and environmental features [25]. They usually use mapping systems to split the map into small segments or grids and then calculate the probability of a crime being committed based on the features of each segment; therefore, risk profiles will be generated for different locations. These methods are also useful to forecast the timing of officer patrols for detecting and deterring criminal activity [26].

The second group is person-based approaches, or offender-based models. These strategies focus on identifying the people who are most likely to be criminals or victims based on their personal information assessment or their history of criminal behavior. These models generate risk profiles of people within the criminal justice system, which are then used by police departments and law enforcement agencies to determine the appropriate actions [25].

Throughout our systematic literature review, we organized the studies based on the techniques that they used in smart policing. These techniques belong to three groups of mapping techniques that involve using statistics, ML, and NLP.

4.1.1. Mapping Techniques

Various mapping techniques are employed to identify crime hotspots, which can be inferred as a basic form of crime prediction. As listed in [27], these techniques include point mapping, thematic mapping of geographic areas, spatial ellipses, grid thematic mapping, and kernel density estimation (KDE).

Spatial ellipses include tools that locate dense concentrations of crime points on a map, known as hot clusters, and then fit a “standard deviational ellipse” to each cluster. These ellipses provide information about the nature of the underlying crime clusters based on their size and alignment [28]. However, criticisms arise due to the need for users to understand the software’s routines, as the lack of guidance on parameter values can lead to ambiguity and variable results. Additionally, the representation of hotspots as ellipses may not accurately reflect the distribution of crime, potentially leading to misleading interpretations [29,30].

Geographic boundary thematic mapping is a method for representing spatial distributions of crime events that involves aggregating crime incidents into predefined geographic units and shading these areas based on the number of crimes within them. However, thematic shading based on boundaries may fail to reveal patterns across and within these units [31]. Despite the limitations, this mapping system is still widely applied in various contexts, including analysis of vehicle theft in relation to land use and crime pattern analysis [29].

Kernel density estimation (KDE) is considered to be the most suitable method for visualizing crime data, due to its availability and accuracy in identifying hotspots, as well as its aesthetic appeal [29,32]. KDE combines the area division in a regular grid of cells and the aggregation of point data within a specified search radius to estimate the probability density of actual crime incidents for each cell by using a kernel function to estimate the probability density of actual crime incidents. This will result in a heatmap that represents the density or rate of criminal events across the study area without being constrained by geometric shapes like ellipses [33].

Despite the popularity of KDE, the selection of a thematic range can be problematic, as agencies often prioritize visual appeal over the validity of the map. This can lead to

variations in maps created from the same data. There are also concerns that maps can be misleading when they are created based on small amounts of data [29].

4.1.2. Machine Learning

In 2012, PredPol, Inc. introduced a predictive analysis platform that provides real-time crime risk information with a precision of 200 meters. This startup gained prominence in predictive policing by offering more than traditional crime hotspot maps [34]. Their method was inspired by earthquake prediction techniques, as researchers observed similarities between crime propagation dynamics and earthquakes [35]. PredPol utilizes stochastic point processes, a statistical physics approach, and a machine learning algorithm to make predictions modeling the distribution of events in time and space. The algorithm is trained based on historical event datasets for each city, and it is regularly updated with new events from the police department on a daily basis [36]. Many similar platforms are in use by police departments throughout the nation, as listed and summarized in Table 1.

More recently, data mining and ML algorithms have played an important role in crime prediction tasks, including predicting crime hotspots and crime categories or identifying criminals and victims. According to studies, predictive policing relies on many data mining and ML techniques, such as classification clustering, and regression, but not all of these techniques perform equally effectively.

Table 1. Platforms that are in use by police departments throughout the nation.

Tool	Reference	Description and Application	Type	Other Technologies in Use	Agencies That Use the Tool
CompStat	[20,37]	Crime data analysis to identify crime trends and patterns within specific districts and guide police departments in addressing crime and allocating resources more efficiently	Location-based	Geographic information system (GIS)	New York Police Department (NYPD)
PredPol	[34,35]	An ML algorithm trained on past crime data alongside hotspot mapping to predict crime risks	Based on crime type, location, and time	Google Maps, GPS, and AVL	More than 60 police departments, including the Los Angeles Police Department and the Atlanta Police Department
HunchLab	[19,38,39]	Uses ML to find crime trends and reflects community needs by giving weight to different types of crimes	Location-based	GIS	Philadelphia Police Department
Palantir	[17]	Makes predictions about crime perpetrators who fit the queries that officers input to the system	Location-based	-	Salt Lake City Police Department
Strategic Subject List	[40,41]	Scoring algorithm to predict risks of offending and involvement in criminal activities based on empirical data, considering factors like the person's criminal record and violence within their criminal network	Person-based	-	Chicago Police Department (CPD)
Beware	[39,42,43]	Individualized risk assessments of potential offenders to inform of potential criminal activities; the risk assessment is based on public arrest records, social media posts, and information compiled by commercial data brokers	Person-based	-	Fresno Police Department

Table 1. Cont.

Tool	Reference	Description and Application	Type	Other Technologies in Use	Agencies That Use the Tool
Domain Awareness System	[44]	An urban network consisting of sensors, databases, devices, software, and infrastructure designed to provide insights and information to officers via smartphones and precinct computers to make them aware of possible criminal activities	A combination of location-based and person-based strategies	Surveillance systems like cameras	New York Police Department (NYPD)
COPLINK	[45,46]	Consists of two components: COPLINK Connect for information sharing between police officers and law enforcement agencies, and COPLINK Detect, which uses AI to find crime patterns	Both location-based and person-based	-	Phoenix Police Department
PRECOBS	[47]	Pre-crime observation system that predicts crimes by mainly consulting the near-repeat hypothesis and a rational-choice-framed conception of offenders that can be translated into algorithms for classifying and evaluating crime risk in geographic areas	Location-based	-	Police departments in Switzerland and Germany

Various studies have compared different algorithms or designed frameworks with the utilization of ML in this context. These algorithms include support-vector machine (SVM), naïve Bayes (NB), artificial neural networks, k-nearest neighbors (KNN), decision tree (DT), and random forest (RF). Table 2 shows a brief summary of these studies, including the algorithms and methods that they have utilized. Table 3 also provides detailed measurements of these studies, including information about the used datasets and the prediction accuracy of each model's performance when applied as reported in the studies.

Accuracy is considered, as most of the methods in the reviewed studies are classification algorithms that are used for predicting crime categories/types or crime hotspots. Random forest, one of the popular methods, is an ensemble learning method used for classification or regression tasks. It generates multiple decision trees by training them on different subsets of the dataset by using the bagging method and random selection of attribute sets. The individual predictions of these trees are then combined and determined by the voting of tree classifiers to generate a final output and reduce the risk of overfitting [48,49].

Table 2. Description summary of studies that use ML algorithms.

Reference	ML Algorithm	Description	Result
[50]	K-means	The resulting clusters plotted on a geospatial plot show the possible crime patterns	
[51]	KNN, RF, SVM, NB, CNN, long short-term memory (LSTM)	Presents a comprehensive comparison of ML algorithms for crime hotspot prediction based on historical data of a large city in Southeast China from 2015 to 2018; they also used built environment data such as road network density and points of interest	LSTM performed better than other models as it extracted the patterns and regularity from historical crime data more accurately; built environment data improved the performance as well

Table 2. Cont.

Reference	ML Algorithm	Description	Result
[52]	LR, DT, RF, multilayer perceptron (MLP), NB, SVM, XGBoost, KNN, LSTM, ARIMA	Performs a comparison between ML algorithms to predict crime hotspots based on historical data and time-series analysis in Chicago and Los Angeles	XGBoost performed better than other algorithms, with 94% and 88% accuracy on the two datasets. LSTM classified crime over different periods, showing that Chicago's crime rate had more variations compared with Los Angeles. The ARIMA model was implemented to analyze the five-year trends of crime rates and hotspots, suggesting moderate variations for Chicago and a decline for Los Angeles
[53]	ARIMA, smoothing exponential methods with SES and HES	An ARIMA time-series model is employed to perform short-term property crime prediction for a city in China based on 50 weeks of property crime data and compared with SES and HES methods	The ARIMA model has higher fitting and prediction accuracy than exponential smoothing
[54]	K-means and NB	Proposed a predictive policing system model focusing on street crime in the Karachi region.	The busiest parts of the cities have the highest rates of crime
[55]	NB and backpropagation (BP) neural network	Explores classification techniques to predict crime categories based on crime datasets collected from socioeconomic and law enforcement data of various states in the USA	NB outperformed the BP algorithm, achieving an accuracy of 90.22% for one group and 94.08% for another
[56]	Linear discriminant analysis (LDA) and KNN	Introduces a new model for crime hotspot prediction that incorporates area-specific heat levels, temporal distances of holidays, and neighborhood attributes to create spatiotemporal characteristics; LDA is used for dimensionality reduction, and KNN is used for prediction	The proposed model performs optimally when analyzing weekly crime statistics
[57]	LASSO feature selection with naïve Bayes and ARIMA model	Proposes a model to predict future crime occurrences at a future time and predict which type of crime may be happening in a given area; it also analyzes crime features including date, time, and geographical factors like latitude and longitude, and employs LASSO feature selection and classification models such as naïve Bayes and SVM to extract insights from the data	The proposed model outperforms SVM, KDE, and deep neural networks in terms of accuracy; however, SVM has the best precision value
[58]	Negative binomial, Poisson regression, and regression models	Crime data of Salinas, California, USA	All three models have similar performance
[59]	SVM, multilayer neural network, LR	Conducts research on how SVM can provide a framework to predict the probability of reincarceration and preforms a comparison among SVM, LR, and neural networks based on a recidivism dataset	SVM can be a reliable method for recidivism prediction, but a combined prediction utilizing all three methods obtains the most flexibility, with enhanced accuracy and effectiveness of crime forecasting
[60]	DT, NB	Predicting crime categories in different states of the USA	DT outperformed NB
[61]	DT J48, NB, SVM, multilayer perceptron	Predicting crime categories	DT outperformed other algorithms

Table 2. Cont.

Reference	ML Algorithm	Description	Result
[62]	DT J48	Suggests a crime prediction prototype model using a decision tree (J48) based on the UCI dataset of “Crime and Communities”	Experimental results indicate that the J48 algorithm achieves an accuracy of 94.25% in predicting crime categories
[63]	DT, NB	Suggests crime category prediction in specific geographical areas using ML algorithms based on historical incident data sourced from the Chicago Police Department’s CLEAR system; both algorithms were applied to the top 9 selected features from the dataset	DT outperformed the NB algorithm in terms of predictive accuracy
[64]	Neural network, NB, RF	Predicting future drug-related crime hotspots	Neural network has a better performance
[45]	NB, DT	Extract rules for classification and prediction of crime and criminality	NB is more reliable
[65]	Linear regression, additive regression, and decision stump	Presents a comparison between the violent crime patterns from the Communities and Crime Dataset provided by the University of California—Irvine repository and actual crime statistical data for the state of Mississippi that were provided by neighborhoodscout.com	Linear regression performs the best
[66]	RF	Long-term crime forecasts for robberies in Dallas in 200 by 200 foot grid cells that allow spatially varying associations of crime generators and demographic factors	RF outperforms risk terrain models and kernel density estimation in terms of forecasting future crimes using different measures of predictive accuracy, but it only slightly outperforms using prior counts of crime
[67]	SVM, KDE, deep neural network (DNN)	Introduces a feature-level data fusion method with environmental context based on a deep neural network that consists of spatial, temporal, environmental context, and joint feature representation layers	Evaluated the performance of SVM, KDE, and their proposed method using accuracy, precision, recall, and area under the curve (AUC). Their DNN-based multimodal data fusion method is a more appropriate method for predicting crime occurrence. The limitation of this model is that it will not work when sufficient data are not provided
[68]	Simple logistic, LR, NB, Bayes net, SVM, DT with C4.5, MLP	Examines the machine learning algorithms and data mining tools in crime analysis in the process of crime prediction and prevention	DT showed promising results, with an accuracy rate of 76%
[69]	Feedforward network, CNN, RNN, recurrent convolutional network	Uses neural network techniques and combines RNN and CNN to predict crime types on different datasets	Evaluated the performance of neural networks, with the following results: feedforward with 71.3% accuracy, CNN with 72.7%, and RNN with 74.1%, and the combination of CNN and RNN with 75.6%.
[70]	Apriori, NB, DT	Applied Apriori to detect frequent crime patterns and NB, and DT to predict the potential crime types	Achieved a prediction accuracy rate of 51% on Denver’s crime dataset and 54% on Los Angeles’ dataset, and provided an analysis study based on the results for each city

Table 2. Cont.

Reference	ML Algorithm	Description	Result
[71]	SVM, NB, KNN	The authors apply ML algorithms to identify hate speech in the context of spiritual belief, emphasizing the importance of monitoring cybercrimes	SVM outperforms NB and KNN in terms of F-score, precision, and recall for sentiment classification and religion classification
[72]	DNN, CNN, RNN	Proposes an intelligent unmanned aerial vehicle system that relies on deep learning algorithms to analyze video data and detect suspicious criminal activities	No performance evaluation is provided; some improvements are suggested for future work, such as battery power and using surveillance-specific algorithms

Clustering methods such as k-means are also popular in crime prediction and analysis. One study provided an ML framework for crime prediction and prevention in big cities using k-means clustering and the naïve Bayes classifier [54]. They showed that, using k-means clustering, they could learn the behavior of the corresponding entity to identify the geospatial region to which it belongs. Using these methods, they identified regions with the highest rates of crime to predict where the next crimes would happen.

Regression methods are used when the objective is to estimate the value of a variable by considering the value of known predictor features. One study performed a comparison between regression models, negative binomial, and Poisson regression, showing that all three of these models perform similarly [58]. In another study [53], the ARIMA model was compared with smoothing exponential methods with SES and HES, where ARIMA showed higher accuracy for crime prediction based on the time series of crime data (including robberies, thefts, and burglaries) derived from the 110 computer-aided dispatch (CAD) recordings of the local police station.

As a relatively new area of application, smart policing technologies are mainly dominated by different types of neural networks, commonly referred to as deep learning methods [69,73–75]. Various types of deep learning methods exist for specific purposes. Convolutional neural networks (CNNs) were designed for image classification tasks like facial recognition, which can also be applied to spatial data, such as maps, treating them as images. In this preprocessing step, CNNs extract essential features from the images, which are then used as predictors in a neural network. Recurrent neural networks (RNNs) were developed to handle pooled cross-section data, enabling the exploitation of temporal structures within the data. Additionally, generative adversarial networks (GANs) can be employed as target hardeners to enhance the security of algorithms that are vulnerable to hacking [76].

In one study [74], researchers used a combination of deep learning and ML methods to design a policing system in Sri Lanka as a mobile application. This system has an automated video surveillance monitoring component that can analyze human activities to identify suspicious behaviors using a CNN model. Also, pretrained state-of-the-art models, including VGG16, InceptionV3, and ResNet-50, are used to obtain high-level feature maps from the final pooling layer output. These extracted features are then fed into an LSTM network to perform the final behavior classifications. In addition, the crime prediction component of the app involves classification algorithms like SVM, DT, RF, and logistic regression (LR) to visually display locations on a map where there is a higher probability of crime occurrence.

Moreover, several studies are dedicated to the application of these algorithms in surveillance technology. These systems, found in public and private locations, allow for simultaneous monitoring of various locations and have evolved significantly over the years given the rising global concerns related to crime and terrorism [77,78]. In [72], the researchers introduced a crime detection system that involves an aerial spy vehicle that resembles the shape of a bird and constantly flies in the sky, capturing images and detecting unusual activities. It relies on deep neural networks (DNNs) to analyze video

data and predict future frames. The process involves converting raw video into individual frames, which are then transformed into grayscale images. CNNs and RNNs are applied to extract features from these images and classify them. The system aims to minimize human intervention and help law enforcement authorities catch criminals effectively.

Furthermore, many studies have focused on the customization of deep neural networks for the real-time detection and classification of weapons during surveillance of criminal activities. These efforts highlight the growing demand for automatic systems in policing, given the increasing rate of crime and the frequent use of handheld weapons like pistols and revolvers in illegal or criminal activities [77,79–86]. Another study proposed a model to detect handguns based on the individual’s pose, utilizing CNNs [87]. Using different architectures of CNN is a common practice for weapon detection in images, as it has shown exceptional performance in object recognition tasks [88]. One of the popular methods used for weapon detection is the YOLO (You Only Look Once) family of CNNs, which has evolved through versions YOLOV1 to YOLOV4. In YOLOV1, there is a single CNN for predicting object bounding boxes in grids [89]. YOLOV2 improved its accuracy with techniques like batch normalization and anchor boxes [90]. YOLOV3 incorporated multilabel classification, prediction of different bounding boxes, and feature pyramid networks. It also introduced the Darknet-53 feature extractor [91]. YOLOV4 further enhanced learning with cross-stage partial connections, Cross mini-batch normalization, mish-activation, mosaic data augmentation, drop block regularization, and Ciou loss for bounding box regression, resulting in improved accuracy and speed [92].

One study introduced a Raspberry-Pi- and cloud-assisted face recognition system for law enforcement agencies, enabling them to securely detect and recognize faces in real-time scenarios. A portable wireless camera was attached to a police officer’s uniform to capture videos, which were processed by the Raspberry Pi for facial detection and recognition. The method employs a bag-of-words model for feature extraction and an SVM for identifying suspects [93]. ML algorithms such as CNN and SVM are applicable in facial recognition, which is a critical area of research, and its applications extend to security, law enforcement, and public surveillance [93–95]. While these algorithms have shown promise in facial recognition, their practicality and effectiveness in real-world law enforcement scenarios remain relatively unexplored.

Table 3. Detailed measurements of studies that use ML algorithms.

Reference	Dataset	No. of Instances	No. of Attributes	Algorithm/Technique	Accuracy (%)
[52]	Los Angeles criminal records (2010–2018) [96]	2.6 million	17	Logistic regression	48
				DT	60
				RF	43
				MLP	84
				NB	71
				SVM	60
				XGBOOST	88
				KNN	89
[52]	Chicago criminal records (2001–November 2019) through the city of Chicago’s data portal website [97]	7 million	22	Logistic regression	90
				DT	66
				RF	77
				MLP	87
				NB	73
				SVM	66
				XGBOOST	94
				KNN	88
[55]	Communities and Crime from the UCI Machine Learning Repository [98]: Group 1, which is classified based on race	2000	128 in total, but only 4 were selected for this study to obtain optimal results	NB	90.22
				BP	94.08

Table 3. Cont.

Reference	Dataset	No. of Instances	No. of Attributes	Algorithm/Technique	Accuracy (%)
[55]	Communities and Crime from the UCI Machine Learning Repository [98]: Group 2, which is classified based on marital status	2000	128 in total, but only 4 were selected for this study to obtain optimal results	NB BP	65.94 65.94
[57]	Chicago crime records through the city of Chicago's data portal website [97]	6,480,461	-	SVM KDE Deep neural network LFSNBC	67.01 66.33 84.25 97.47
[59]	Data1978	4618 (9327 in total, but 4709 instances were excluded due to missing information)	-	LR SVM Neural network	-
[59]	Data1980	5739 (9549 in total, but 3810 instances were excluded due to missing information)	-	LR SVM Neural network	-
[60]	Communities and Crime from the UCI Machine Learning Repository [98]	1994	128	DT NB	83.9519 70.8124
[61]	Communities and Crime from the UCI Machine Learning Repository [98]	1994	128	DT J48 NB MLP SVM	100 89.6104 100 92.2078
[62]	Communities and Crime from the UCI Machine Learning Repository [98]	1994	12	DT J48	94.2528
[63]	Chicago incident reports from 2013 to 2017 [99]	12,109	18	NB DT	83.33 91.59
[65]	Communities and Crime Unnormalized Dataset	2215	147 in total (4 non-predictive features, 125 predictive features, and 18 potential goal features), but 9 attributes related to violent crimes were selected for this study	Linear regression- Additive regressionDecision stump	Not defined
[65]	Mississippi 2013 Crime Dataset [100]	89,714 recorded crimes, but 8214 records were selected for this study	-	Linear regression- Additive regressionDecision stump	Not defined
[66]	Crime data related to robberies reported from incident-level data and geocoded to the address level on the Dallas Open Data portal [101]	12,613	-	RFKDECounting prior crimes Risk terrain modeling	-

Table 3. Cont.

Reference	Dataset	No. of Instances	No. of Attributes	Algorithm/Technique	Accuracy (%)
[67]	Chicago crime records for 2014 through the city of Chicago's data portal website [97], American Community Survey data, weather data from Weather Underground [102], and environmental context information from image data using Google Street View [103]	274,064 crime cases from Chicago crime records, 801 census tracts from the American Community Survey	-	SVM KDE Deep neural network	67.01 66.33 84.25
[69]	Chicago crime records through the city of Chicago's data portal website [97], along with census data through the United States Census Bureau and weather data through the National Oceanic and Atmospheric Administration	6 million records	-	Feedforward CNN RNN RNN + CNN	71.3 72.7 74.1 75.6
[69]	Portland crime data through the National Institution of Justice Real-Time Crime Forecasting, along with census data through the United States Census Bureau and weather data through the National Oceanic and Atmospheric Administration	-	-	Feedforward CNN RNN RNN + CNN	62.2 62.9 63.8 65.3
[70]	Denver crimes dataset (2010–2015) [104]	333,068	19	NB DT	51 42
[70]	Los Angeles crimes dataset (96% for 2014 and 4% for before 2014) [105]	243,750	14	NB DT	54 43

4.1.3. Natural Language Processing

Most police departments use electronic systems for crime reporting that have replaced the traditional paper-based crime reports. When a crime is recorded by police, situational and behavioral details describing the incident are documented in a free-text narrative report. These crime reports typically contain information such as the type of crime, date/time, location, and information about the suspect, victim, and witness(es), in addition to the narrative or description of the crime. The challenge in mining crime data often comes from the narrative part, as converting them into data mining attributes is not always an easy job [50]. Some studies have shown that, by means of NLP, these documents can be more useful for administrative and investigative tasks in smart policing [106]. NLP is a subset of AI and ML that includes approaches to analyze natural language in text or speech [107].

Police narrative reports are noisy, as they include grammatical mistakes, misspellings, acronyms, and informal language. Also, as other entities such as crime type names or vehicles also exist in these reports, general named-entity recognition tools may not be effective. Additionally, they include sensitive data, including the personal information of victims or criminals. Therefore, NLP models to analyze crime data in these reports should be trained on various data addressing these challenges. Additionally, police agencies often lack the expertise and resources to conduct detailed analyses or securely share data for academic research.

As mentioned earlier, ML has been recognized as a valuable tool in the field of criminology. However, according to a recent review on the intersection of crime and AI, there is a lack of research specifically focusing on NLP in this literature, particularly in relation to police free-text data analysis. In this section, our focus is specifically on analyzing free-text police data [108].

Existing analysis of free-text crime data often revolves around unsupervised learning and crime linkage [8]. Crime linkage aims to identify crimes committed by the same individual(s). Notable studies using unsupervised learning and NLP with police free-text data include [109] and [110], which explored how crimes can be grouped based on their characteristics and how they were committed. Other studies, like [111,112], use unsupervised NLP techniques to cluster crimes to inform policing strategies in different areas.

There have also been efforts to extract specific information directly from police free-text data, such as exploring the relationship between mental health and types of domestic violence through rule-based information extraction [113,114]. However, this approach requires substantial effort in building rules and dictionaries, making it challenging for routine adoption.

Additionally, many studies focus on analyzing data from social media platforms such as Twitter. For example, a study has hypothesized that language usage on Twitter can be a valuable measure to predict crime rates in cities. They used the WEKA preprocessing toolkit and SVM to analyze and classify Twitter data [115].

Other studies have explored Twitter-based prediction of criminal incidents, specifically focusing on hit-and-run crimes [97,116]. Their approach involved semantic analysis of tweets through semantic role labeling to extract events mentioned in tweets. They then employed latent Dirichlet allocation for event-based topic extraction, revealing hidden relationships between major events and observable events reported in tweets. The predictive model itself relies on a generalized linear regression framework to predict whether an incident will occur on the following day based on the information gleaned from tweets.

One of the common NLP techniques used in smart policing, especially in writing police reports, is information extraction, including named-entity recognition (NER), which aims to detect named entities such as people, places, organizations, and dates and extract specific crime elements from reports and data. NER enables better problem grouping and improves information availability, which is often lacking in structured formats. By automating the extraction of detailed information from crime reports, NER significantly reduces the analysis time, allowing police analysts to respond effectively. Studies that utilize information extraction and NER for crime data analysis are listed in Table 4.

In [117], four main approaches for NER are listed (lexical lookup, rule-based, statistics-based, and ML), while most of the existing NER systems are based on more than one of these approaches. Another study proposed an information extraction method using NER that outperformed Linguakit, a multilingual toolkit developed for NLP that contains NER, and RAPORT, which is a Portuguese question-answering system that uses NLP and NER [118].

Table 4. Studies that use NLP techniques.

Reference	Data Source(s)	Description	Result
[115]		Text analysis and classification using the WEKA toolkit and SVM	
[116]	Twitter data in addition to 290 incident records collected from local law enforcement agencies in Charlottesville, Virginia	Explores Twitter-based prediction of criminal incidents, with a focus on hit-and-run crimes, using NLP techniques such as sentiment analysis and event extraction. A linear regression model is also used to predict if a crime will occur in the following days based on information extracted from the tweets	The model's performance was evaluated using a receiver operating characteristic (ROC) curve. The results indicated that data from social media platforms such as Twitter could be a valuable resource for predicting criminal incidents, but there are areas for improvement and further research, especially considering the temporal aspect of event descriptions and feature selection methods
[118]	Portuguese narrative police reports	Presents a system that uses information retrieval techniques to extract, transform, clean, load, and find a connection between police reports collected from different sources to identify relevant entities within the extracted information	The proposed model outperformed Linguakit and RAPPORT in terms of the F-score
[119]	Mozenda Web Screen Scraper tool and 4 online newspapers: <i>Otago Daily Times</i> , <i>Zealand Herald</i> , <i>Sydney Morning Herald</i> , and <i>The Hindu</i>	Proposed a crime information extraction system using NER and a conditional random fields (CRF) machine learning approach to identify locations in sentences and classify them based on online newspapers by focusing on information related to the theft crime	The model was evaluated based on four newspaper articles from three countries, resulting in accuracy of 84% to 90% for articles from New Zealand and 73% to 75% for articles from India and Australia
[120]	Malaysian newspapers and social media sites	Introduced an ensemble framework for crime information extraction from the web using NER and classification algorithms including NB, SVM, and KNN, along with a weighted voting ensemble method to combine them	The proposed model outperformed the baseline models, with an F-score of 89.48% for identifying crime types and 93.36% for extracting crime-related entities
[121]	News articles related to identity theft on the internet found by search engines and annual identity theft reports	Proposed an approach to analyze criminal behaviors and predict future trends of identity theft and fraud using NLP methods and information extraction, including NER and part-of-speech tagging based on raw text from news articles on the web. The Identity Threat Assessment and Prediction (ITAP) algorithm, designed in a modular pipeline, collects news stories, preprocesses them, extracts named entities, categorizes them, and creates identity theft records	Around 3500 identity theft news stories were collected, their text was cleaned, and named entities were extracted and categorized. These categories formed identity theft records, which were then used for various analyses, such as identifying affected groups, assessing risk for specific PII attributes, tracking occurrence frequency across different sectors and locations, evaluating potential financial impacts, and tracking changes over time
[122]	A set of crime reports related to internet fraud on the official website of the Dutch police (each report contains 1–5 sentences and 85 tokens on average)	Evaluates the standard NER algorithm, named Frog, for the Dutch language based on a manually annotated corpus collected from 250 complaints reports from the Dutch police; it discusses confusion in entity type assignment and recall errors, and proposes ways to improve performance	The current Dutch NER algorithm performs inadequately on unedited free-entry data. The significance of this depends on the purpose of entity recognition, e.g., law enforcement seeks relevant information, while linguistics aims for named-entity identification, so different types and assignments matter, and domain-specific roles demand further processing

Table 4. Cont.

Reference	Data Source(s)	Description	Result
[123]	-	Proposed a method for extracting valuable information about suspects' hard drives and social networks to discover criminal communities and analyze their relations	The method efficiently identified criminal communities and their interlinked subgroups, offering a detailed view of network structure, crucial for criminal network analysis; it also received positive feedback from a Canadian law enforcement unit's digital forensics team
[117]	A set of police narrative reports provided from the Phoenix Police Department database	Presents a neural-network-based entity extractor by using NER techniques to detect valuable entities such as person names, addresses, narcotic drugs, and vehicle names in police reports	The system achieved promising precision and recall rates for person names and narcotic drugs but performed less effectively for addresses and personal properties
[124]	Texts on the web	Proposed a semantic NLP model to develop systems that extract crime information from unstructured text in a collaborative web environment. The framework centers around a semantic inferential model (SIM)-based NLP module	This framework's performance was demonstrated through the creation of "WikiCrimesIE," a tool for extracting crime-related information from text on the web, which gained an F-score of 78% for crime extraction and 70% for crime type identification
[125]	Chinese criminal investigation notes, online news on the internet, and litigation data	Introduces a method for criminal information analysis and relation visualization by utilizing entity extraction techniques and part-of-speech (POS) tagging based on Chinese criminal text	By forming term networks based on documents from sources like criminal investigation notes, news, and litigation data, this method enhances the visualization of detailed information and hidden relationships, enabling efficient exploration of potential criminal activities
[126]	65 Arabic crime articles with a total of 13,300 words	Introduces a rule-based NER to identify and classify named entities in Arabic crime text as it applies syntactical rules such as sentence splitting, tokenization, and POS tagging	The system achieved 90% accuracy, showing effectiveness and satisfactory performance. The paper outlines plans to integrate the rule-based system with machine learning techniques and embed it within a crime analysis framework
[127]	Crime news articles represented in html format collected from the Malaysian National News Agency (BERNAMA)	Introduces a method to extract information on nationalities from crime news in Malaysia by applying NER using gazetteers and rule-based extraction. The system is composed of three modules: direct extraction, indirect extraction, and victim–suspect reference identification	The method's performance was evaluated based on a manual extraction system and showed an F-score of 70%. The authors also highlighted challenges with punctuation and nationality indicators causing the system to miss certain references or extract incorrectly, as well as difficulties in identifying implicit state markers for victims or suspects
[128]	Crime news from online sources and crime records for 2001 to 2014 provided by the National Crime Records Bureau	Presents an Android application called Reach 360, designed to offer alerts and support in dangerous situations, including features such as alerting contacts, demonstrating crime hotspots via heatmaps, and forecasting crimes based on crime news using machine learning. NLP tasks such as sentence segmentation, word tokenization, POS, and NER are used to process crime news	Multilayer perceptron performed better than logistic regression and RF in terms of accuracy for crime forecasting. The study does not provide other specific details on the performance evaluation of their application; it mainly focuses on introducing its features, the methodology behind it, and its potential to address safety concerns and forecast crimes

Table 4. Cont.

Reference	Data Source(s)	Description	Result
[129]	Official data of crime records from Porto's Public Security Police between January 2016 and December 2018	Explores the application of mapping techniques, NLP, and ML models such as SVM, LR, DT, and RF to analyze crime patterns and predict crimes. The study collected tweets related to insecurity around crime locations and performed topic modeling and sentiment analysis. Latent Dirichlet allocation (LDA) was also used to classify tweets into topics, while sentiment analysis identified positive and negative sentiments related to crime	This method identified crime patterns and crime hotspots in downtown Porto and emphasized the importance of crime trend forecasting for resource allocation. The study does not provide details on the evaluation of the used models
[130]	Patch Hate Crime dataset, <i>New York Times</i> news reports	Introduces a framework to address the problem of hate speech on social media and its connection to hate crime with a combination of event extraction through NLP, time-series analysis, and regression analysis. The event-related factors extracted using event extraction are integrated into a regression model. These factors, along with other predictive features, are used to predict hate crime trends	Various models were applied to forecast hate crime trends, and the results were compared. Regressive models outperformed the ARIMA model, with models including event-related variables performing better
[131]	Twitter posts by users in the United Kingdom between October 2015 and October 2016	Presents a comprehensive study of online antagonistic content on Twitter that involved data collection from Twitter	The authors developed a supervised machine learning classifier with a bag-of-words model to identify antisemitic content, providing an analysis of the production and propagation of antagonistic content
[132]	A corpus of two million downloaded tweets	Introduces an intelligent system used by the Spanish National Office Against Hate Crimes to identify and monitor hate speech on Twitter. The system makes use of NLP methods including lemmatization, stop-word removal, and POS tagging for preprocessing tweets, and then classifies them using MLP and LSTM	The authors evaluated 19 different strategies, each comprising various combinations of features and classification models. Ultimately, the top-performing model, achieving an AUC of 0.828, leveraged word embeddings, emojis, and token expressions and further enhanced them through text frequency-inverse document frequency. This approach outperformed the existing models in the literature.
[71]	Twitter posts	Applies ML algorithms to Twitter posts for text classification and sentiment analysis to analyze hate speech and hateful sentiment in the context of spiritual belief	SVM outperformed NB and KNN in terms of F-score, precision, and recall for sentiment classification and religion classification

An online reporting system was developed in [133], combining information extraction and named-entity recognition with the principles of cognitive interview to retrieve information from police and witness narrative reports, with a significantly high precision rate of 94% for police narratives and 96% for witness narratives, and a recall rate of 85% for police narratives and 90% for witness narratives. The authors emphasized that utilizing information extraction methods such as named-entity recognition in crime data can help investigators to effectively collect and extract more information, especially from individuals who may be hesitant or embarrassed to report incidents [134].

Several studies demonstrate the effective fusion of NLP and ML techniques [115,116,128,129]. In [128], with a primary emphasis on enhancing women's safety, the authors introduce an Android mobile application that can send alerts to users about locations where a crime has recently happened through a heatmap visualization. They use NLTK to extract information from the web through NLP tasks such as NER, part-of-speech tagging, and tokenization. Additionally, they take advantage of the MLP algorithm to forecast crime. An interesting use-case study also provides a comprehensive approach to crime analysis by integrating mapping techniques such as KDE and hotspot analysis, ML models, and NLP to understand crime patterns and forecast crime occurrence [129]. They applied NLP methods such as topic modeling and sentiment analysis to tweets related to crime.

As demonstrated by researchers, hate speech crime detection can be considered as another application of smart policing where using NLP techniques alongside ML methods is common. One study introduced a framework to address the problem of hate speech on social media and its connection to hate crimes [130]. The authors used NLP techniques for event extraction and a regression model based on multi-instance learning to extract hate crime events from the *New York Times*. In [131], the researchers utilized the SVM model combined with a bag of words to perform text classification on Twitter posts and analyze online antisemitism patterns, emphasizing the value of collective efficacy in countering online hate speech.

Another paper introduced "HaterNet", a novel classification approach that combines an LSTM neural network with an MLP, with a high AUC of 0.828 for identifying and monitoring hate speech on Twitter [132]. The authors took advantage of NLP methods including lemmatization, stop-word removal, and POS tagging for preprocessing tweets, so they were presented as a vector of unigrams based on frequency and word embeddings. While detecting hate speech as a crime falls under the broad umbrella of smart policing, it is a specific focus area due to the unique challenges and consequences associated with hate speech. Smart policing can help authorities respond more effectively to hate speech, prevent escalation to hate crimes, and maintain public safety.

Furthermore, with the recent rise and popularity of generative AI and large language models such as GPT 3.5, there is a controversy about their usage in smart policing and other applications, but there are only a few studies considering the use of generative AI or customizing language models for smart policing purposes. By means of NLP models, these AI tools have shown significant success in various tasks and domains, including healthcare and medicine [135], reducing the need for extensive preprocessing of text. As mentioned in [106], while large language models hold promise for supporting policing through NLP, ethical challenges will be raised. In the following section, we address RQ2 by explaining these challenges and concerns of using AI.

4.2. Addressing RQ2

Several studies have analyzed the use of AI technologies in smart policing from different perspectives. Researchers have pointed out that AI is changing policing just like other aspects of society, but the concerns and challenges may differ due to the special role of police in societies [16,136]. Therefore, it is essential to evaluate the proposed solutions and how much they are going to be used by law enforcement agencies. Despite the powerful and fast tools that AI offers for policing tasks, utilizing them still raises ethical concerns about possible biases. According to these concerns, experts have argued that predictive algorithms are tools to assist law enforcement by enhancing their judgment, not to replace them [137,138]. Additionally, studies suggest that the legal and ethical complexities of using ML algorithms in smart policing demand continuous attention. Therefore, a collaborative, multidisciplinary approach involving policing, computer science, law, and ethics experts should address the challenges and operational requirements of using such algorithms in smart policing by defining standards for transparency, intelligibility, and ethical considerations [139,140].

Transparency, in this context, refers to the visibility and accessibility of the used algorithm's source code and parameters [141]. Intelligibility, on the other hand, pertains to the degree to which the code or disclosed information sufficiently explains how the model operates in practice, while auditability allows human observers to retroactively examine how the tool arrived at a certain decision [140].

Studies also recommend that for AI algorithms to be valuable in smart policing and law enforcement, they must not only improve their efficiency and accuracy but also be perceived as fair in their recommendations or decision-making [142]. Data retrieval from these algorithms depends on the data that they are fed or trained with. As [143] explains, police play a special role in creating their data. The algorithms are trained based on historical datasets, which means that they can learn the biases and patterns in the data created by human decisions, so if there is a bias in the data themselves, this bias also exists in the functionality of the algorithm. On the other hand, another study argues that depending solely on human oversight of automated systems, known as "human-in-the-loop" approaches, is deficient. Instead, it emphasizes the importance of transparency and accountability in the training phase of machine learning algorithms, especially during their parameterization. In addition, it explains that by using such methods, traditional accountability linked to a public official's decision-making has now shifted to those who design machine learning systems, collect the datasets, and implement the system within the framework. In other words, just having accurate predictions does not necessarily lead to improved smart policing performance. The authors of [139] highlighted the need for evaluating the fairness of algorithms and AI tools used in smart policing.

According to several studies [139,142,144], bias in AI algorithms is defined as using data or algorithmic outputs that lead to unethical discriminatory effects on individuals and communities, or when the collected data are insufficient or unrepresentative. Crime data themselves may be biased, reflecting past police actions rather than true crime patterns, so striking the right balance between predictive power and fairness is challenging. Developing and implementing fair and transparent algorithms requires interdisciplinary collaboration between police, mathematicians, computer scientists, data scientists, and legal experts.

Additionally, using AI in smart policing raises questions about proportionality and the balance between individual rights and public purposes, and about how much the police should inform the public about the AI that they use [16]. In any event, each case of algorithmic implementation must be carefully reviewed, and ongoing attention and vigilance are needed to ensure fairness as the datasets are continually updated and revised.

The authors of [106,145] state that there are three main reasons for biases: *data coverage*, which means that police may not be aware of all crimes happening because not all crimes are reported to the police, and this reporting gap may lead to biases in specific regions (for example, regions with a higher presence of police may have a higher rate of crime or arrests) [146]; *data richness*, as the accuracy of the extracted data from police free-text relies heavily on the quality of the original reports, and their possible systematic imbalances specific to different areas and communities can lead to biases in AI algorithms; and *algorithmic bias*, which arises when certain crime descriptions are not well understood by certain models, especially if the original training data for the language models lack exposure to reports with such unusual language.

To address these challenges, [106] suggests conducting research on the richness and quality of information that is recorded about a crime incident, criminals, and victims, in addition to reviewing and considering all available models for different crimes and incidents to make sure that information is not misrepresented to the algorithms. In addition, it suggests that the technical teams should work closely with police partners while sharing their data with additional security measures and their concerns. This approach provides a promising start to understanding the potential utility of AI in smart policing.

Moreover, another study [142] outlined different metrics proposed by [3] and [147–152] to measure fairness, which should be considered while designing predictive systems and algorithms in smart policing. These metrics include classification parity, which considers

an algorithm to be fair if it equally predicts positive classification for both privileged and disadvantaged groups; calibration, which assesses the fairness of the algorithms by ensuring that subjects in both groups have the same likelihood of positive classification for any predicted probability; equalized odds, which requires equal likelihood of both positive and negative outcomes for both groups; and equal opportunity, which ensures that the predictor predicts positive classification for both groups with the same likelihood. It also defines fairness through awareness, which focuses on treating similar individuals with similar outcomes, and counterfactual fairness, which ensures that a prediction algorithm treats an individual equally regardless of the group they belong to.

In general, most studies emphasize the need for careful consideration regarding AI and its application in smart policing, so as to prevent unjust and unethical impacts. Understanding the computational techniques and datasets used in designing such systems is crucial, as biases within the data can lead to unfair outcomes. Moreover, as mentioned in [153], the use of AI tools can influence people's beliefs and practices, potentially prejudicing and disrespecting individual rights and dignity. Therefore, they proposed the ethics-of-care approach in AI system design to address these issues, aiming to mitigate significant flaws and potential harms in AI systems that can affect people's lives and societies. This ethical approach can extend beyond smart policing and find relevance in various applications of AI for consequential decision-making.

5. Next-Generation Smart Policing

Mobile Innovations Corporation offers an electronic pocket notebook (EPNB) application designed and implemented on Microsoft Azure to empower police officers by replacing traditional pen-and-paper methods and enhancing interconnectivity among law enforcement professionals. This solution facilitates the secure and comprehensive collection of data through mobile devices, allowing officers to integrate text, audio, pictures, statements, and tickets with their narrative reports, thereby creating a documentation system.

With the development of AI generative tools, large language models, and chatbots such as ChatGPT, there is a need for conducting research that delves into their applications in the realm of smart policing. Specifically, the focus of this research was on the integration of these advanced technologies within the EPNB framework. Such integration holds the potential to improve how law enforcement operates.

For this purpose, we used Azure OpenAI Studio to fine-tune the OpenAI API. The OpenAI API includes a set of models with different features, and they can be customized for specific tasks with few-shot prompting and fine-tuning. The Azure OpenAI Service provides REST API access to language models such as GPT-35-Turbo, which is optimized for conversational interfaces. We tried different examples and scenarios to test the named-entity recognition and summarization abilities of this model. Then, by means of prompt engineering, we customized the tasks for the chatbot on the Chat Playground of Azure OpenAI Studio using the following system message:

"You are an AI assistant that helps police officers to fill report template files. You will be given a narrative report from a police officer, you have to extract the name of the criminal, the name of the victim, their age, race, sex, type of incident/occurrence, charges, the amount of the charges, date and time, location, addresses, and other related name entities and statue of the case and put them into a JSON format."

For example:

```
[[
  "criminal name": "Value1",
  "criminal age": "Value2",
  "location": "Value3",
  # ...
]]
```

If any of this information is not defined in the report just leave it blank. You also need to summarize the narrative report and put it into “summary” in the same JSON format file.”

This chatbot receives a narrative report as an input and then extracts information such as date/time, location, criminal’s name, victim’s name, etc. Then, it generates a JSON format text including this information. The output JSON file is used to fill the incident report template. Figure 1 shows a schema of the application.

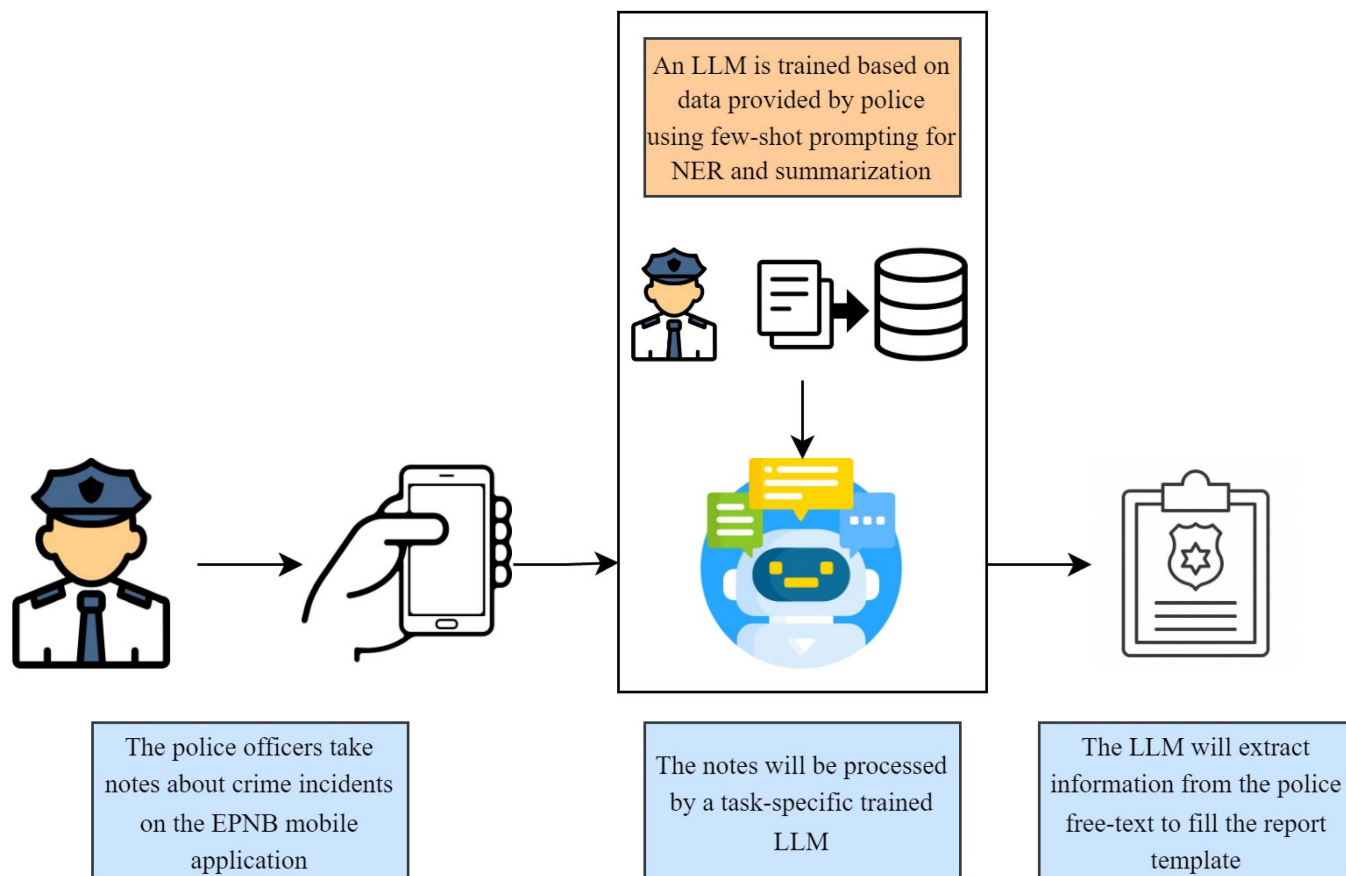


Figure 1. A simplified schema of the designed application for Mobile Innovations. The EPNB application is integrated into Microsoft Azure’s cloud, which also offers services to use advanced technologies such as OpenAI and the Azure Language Service through API calls.

As we tested different scenarios using this AI assistant, it showed great performance when comparing the results with police reports. This is a test case of using large language models in smart policing and how AI can be used in document management; however, there is still room for improvement and research due to the lack of available data.

6. Discussion

The landscape of AI and its applications in smart policing presents opportunities that hold the potential to enhance law enforcement practices. While acknowledging that each application within smart policing presents its own unique set of challenges, providing a comprehensive exploration of these challenges and their solutions within a single study is inherently intricate. Therefore, our focus was on reviewing methods with proven statistical reliability, aiming to cover a comprehensive and representative range within the scope of a literature review. Based on our survey, most of the current studies focus on using machine learning algorithms in smart policing applications such as crime prediction and the detection of suspicious activities through surveillance cameras. Additionally, some studies present NLP methods such as sentiment analysis, text classification, and information extrac-

tion systems to detect hate speech crimes and analyze social media data for efficient crime analysis and criminal document management. However, future research could explore more advanced NLP techniques for extracting information from social media and police narrative reports. Leveraging deep learning models like transformer-based architectures or large language models could enhance the accuracy and depth of information extraction from free-text data.

In this study, we showed a test case of large language models in smart policing, but the integration of large language models into smart policing raises an urgent need for comprehensive evaluation in terms of technical feasibility and ethical considerations. As these models learn from a large amount of data, there is a potential for providing biased results that reflect the biases present in the data. Therefore, it is suggested to initiate a process of gathering feedback from police officers, law enforcement agencies, and even the related communities, so that we can evaluate these models with more confidence. The feedback-driven evaluation would aid in understanding the possible biases in AI tools and the ethical implications associated with their deployment in smart policing. Future research in this context could focus on the development of algorithms that actively detect biases in smart policing algorithms. These algorithms could be designed to recognize and minimize impacts on social groups, suggesting fair results and reducing the potential for discriminatory outcomes. By designing such smart systems, researchers can pave the way for the responsible and effective integration of AI in law enforcement practices. This would not only enhance the credibility of smart policing but also build trust between law enforcement and the communities that they serve.

Ethical considerations can affect the future of AI in smart policing, so creating specific ethical frameworks that address such challenges posed by generative AI and large language models is crucial. As discussed in several studies, these frameworks should center around transparency, accountability, and fairness by incorporating human-centered design principles that engage both law enforcement personnel and the involved social communities, such as technologies that align with their real-world needs. This approach will guide the development and deployment of AI tools, thus mitigating concerns of overreliance on automated systems in the decision-making process.

Moreover, a global perspective is essential in understanding how each country adopts AI strategies within its own legal and social contexts for smart policing. A comparative analysis would shed light on successful practices, potential pitfalls, and cultural norms that influence the adoption and implementation of AI technologies. Such insights could aid in the creation of adaptable and context-aware frameworks that consider the complexities of different jurisdictions and societies.

7. Conclusions

This systematic review explored studies that propose ML and NLP approaches to use in policing, in addition to summarizing the potential challenges and issues regarding the use of these methods. Predictive policing and other AI technologies have shown the potential to be faster than traditional response-based policing, as exemplified by their effectiveness in crime analysis, which could be helpful in monitoring criminal activities and allocating safety resources more accurately. However, its success in producing accurate results and its impact on crime rates depend on considering ethical concerns and understanding crime incidents, which can be resource-intensive to extract from police administrative free-text data. Based on our systematic literature review, ML and NLP offer possible solutions to ease the analytical burden for police, enabling their wider adoption. This widespread and careful adoption of smart policing could have a positive impact on society by reducing opportunities for crime and the resulting harm from victimization and offending.

While ML and NLP show promise, there are challenges, including the technical expertise required to use such models and the need to consider ethical issues and address potential biases. We listed the defined measurements to evaluate the ethics of using ML and NLP. Police agencies often lack the necessary expertise, and private companies may

prioritize protecting their technologies over transparency. Therefore, studies suggest that it falls upon the academic community to explore how these technologies can support policing efforts and address these challenges to avoid negative outcomes. If implemented properly, AI can empower policing techniques, especially predictive policing, leading to more efficient monitoring of criminal activities and mitigation of the associated harms.

Author Contributions: Writing—original draft preparation: P.S.; supervision and writing—review and editing: Q.H.M. and A.A.; resources and validation: G.B. and I.B. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by a Mitacs Accelerate collaborative research project with industry partner Mobile Innovations.

Data Availability Statement: Not applicable.

Conflicts of Interest: Gary Bauer and Ian Bowles were employed by the company Mobile Innovations Corporation, Niagara Falls, Ontario, L2G 0M5, Canada. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Camacho-Collados, M.; Liberatore, F. A decision support system for predictive police patrolling. *Decis. Support Syst.* **2015**, *75*, 25–37. [\[CrossRef\]](#)
2. Gable Cino, J. Deploying the secret police: The use of algorithms in the criminal justice system. *Ga. Stet Univ. Law Rev.* **2018**, *34*, 1073.
3. Mehrabi, N.; Morstatter, F.; Saxena, N.; Lerman, K.; Galstyan, A. A survey on bias and fairness in machine learning. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–35. [\[CrossRef\]](#)
4. Ferguson, A.G. Predictive policing and reasonable suspicion. *Emory LJ* **2012**, *62*, 259. [\[CrossRef\]](#)
5. Page, M.J.; Moher, D.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. *BMJ* **2021**, *372*, n160. [\[CrossRef\]](#) [\[PubMed\]](#)
6. Saravanan, P.; Selvaprabu, J.; Arun Raj, L.; Abdul Azeez Khan, A.; Javubar Sathick, K. Survey on crime analysis and prediction using data mining and machine learning techniques. In *Advances in Smart Grid Technology: Select Proceedings of PECCON 2019—Volume II*; Springer: Singapore, 2021; pp. 435–448.
7. Carnaz, G.; Quaresma, P.; Beires Nogueira, V.; Antunes, M.; Fonseca Ferreira, N.N. A review on relations extraction in police reports. *New Knowl. Inf. Syst. Technol.* **2019**, *1*, 494–503.
8. Hassani, H.; Huang, X.; Silva, E.S.; Ghodsi, M. A review of data mining applications in crime. *Stat. Anal. Data Min. ASA Data Sci. J.* **2016**, *9*, 139–154. [\[CrossRef\]](#)
9. Mandalapu, V.; Elluri, L.; Vyas, P.; Roy, N. Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future Directions. *IEEE Access* **2023**, *11*, 60153–60170. [\[CrossRef\]](#)
10. Nicholls, J.; Kuppa, A.; Le-Khac, N.-A. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access* **2021**, *9*, 163965–163986. [\[CrossRef\]](#)
11. Thomas, A.; Sobhana, N. A survey on crime analysis and prediction. *Mater. Today Proc.* **2022**, *58*, 310–315. [\[CrossRef\]](#)
12. Maliphol, S.; Hamilton, C. Smart Policing: Ethical Issues & Technology Management of Robocops. In Proceedings of the 2022 Portland International Conference on Management of Engineering and Technology (PICMET), Portland, OR, USA, 7–11 August 2022; pp. 1–15.
13. Raaijmakers, S. Artificial intelligence for law enforcement: Challenges and opportunities. *IEEE Secur. Priv.* **2019**, *17*, 74–77. [\[CrossRef\]](#)
14. Baek, M.-S.; Park, W.; Park, J.; Jang, K.-H.; Lee, Y.-T. Smart policing technique with crime type and risk score prediction based on machine learning for early awareness of risk situation. *IEEE Access* **2021**, *9*, 131906–131915. [\[CrossRef\]](#)
15. Elluri, L.; Mandalapu, V.; Roy, N. Developing machine learning based predictive models for smart policing. In Proceedings of the 2019 IEEE International Conference on Smart Computing (SMARTCOMP), Washington, DC, USA, 12–15 June 2019; pp. 198–204.
16. Joh, E.E. Artificial intelligence and policing: First questions. *Seattle UL Rev.* **2017**, *41*, 1139.
17. Yang, F. Predictive policing. In *Oxford Research Encyclopedia of Criminology and Criminal Justice*; Oxford University Press: Oxford, UK, 2019.
18. Matsueda, R.L.; Kreager, D.A.; Huizinga, D. Deterring delinquents: A rational choice model of theft and violence. *Am. Sociol. Rev.* **2006**, *71*, 95–122. [\[CrossRef\]](#)
19. Brayne, S.; Rosenblat, A.; Boyd, D. Predictive Policing. *Data Civ. Rights New Era Polic. Justice* **2015**. Available online: https://datacivillights.org/pubs/2015-1027/Predictive_Policing.pdf (accessed on 1 October 2023).

20. Willis, J.J.; Mastrofski, S.D.; Weisburd, D. Making sense of COMPSTAT: A theory-based analysis of organizational change in three police departments. *Law Soc. Rev.* **2007**, *41*, 147–188. [\[CrossRef\]](#)
21. Cardon, D. *Deconstructing the Algorithm: Four Types of Digital Information Calculations*; Routledge: London, UK, 2016.
22. Dourish, P. Algorithms and their others: Algorithmic culture in context. *Big Data Soc.* **2016**, *3*, 2053951716665128. [\[CrossRef\]](#)
23. Kitchenham, B.; Brereton, O.P.; Budgen, D.; Turner, M.; Bailey, J.; Linkman, S. Systematic literature reviews in software engineering—A systematic literature review. *Inf. Softw. Technol.* **2009**, *51*, 7–15. [\[CrossRef\]](#)
24. Rajaei, M.J.; Mahmoud, Q.H. A Survey on Pump and Dump Detection in the Cryptocurrency Market Using Machine Learning. *Future Internet* **2023**, *15*, 267. [\[CrossRef\]](#)
25. Bertovskiy, L.V.; Novogonskaya, M.S.; Fedorov, A.R. Predictive Policing: High-tech Modeling as a Method to Identify Serial Killers. *Kutafin Law Rev.* **2022**, *9*, 329–342. [\[CrossRef\]](#)
26. Shapiro, A. Reform predictive policing. *Nature* **2017**, *541*, 458–460. [\[CrossRef\]](#)
27. Chainey, S.; Tompson, L.; Uhlig, S. The utility of hotspot mapping for predicting spatial patterns of crime. *Secur. J.* **2008**, *21*, 4–28. [\[CrossRef\]](#)
28. Block, R.; Perry, S. STAC News. *Ill. Crim. Justice* **1993**, *1*, 4–28.
29. Eck, J.; Chainey, S.; Cameron, J.; Wilson, R. *Mapping Crime: Understanding Hotspots*; National Institute of Justice: Washington, DC, USA, 2005.
30. Ratcliffe, J.; McCullagh, M. Crime, repeat victimisation and GIS. *Mapp. Anal. Crime Data* **2001**, 61–92. [\[CrossRef\]](#)
31. Williamson, D.; McLafferty, S.; McGuire, P.; Ross, T.; Mollenkopf, J.; Goldsmith, V.; Quinn, S. Tools in the spatial analysis of crime. Mapping and analysing crime data. *A. Hirschfield K. Bowers. Lond. New York Taylor Fr.* **2001**, *1*, 187.
32. Rosenblatt, M. Remarks on some nonparametric estimates of a density function. *Ann. Math. Stat.* **1956**, *1*, 832–837. [\[CrossRef\]](#)
33. de Queiroz Neto, J.F.; dos Santos, E.M.; Vidal, C.A. Mskde-using marching squares to quickly make high quality crime hotspot maps. In Proceedings of the 29th SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI), Sao Paulo, Brazil, 4–7 October 2016; pp. 305–312.
34. Benbouzid, B. Values and Consequences in Predictive Machine Evaluation. A Sociology of Predictive Policing. *Sci. Technol. Stud.* **2018**, *31*. Available online: <https://ssrn.com/abstract=3123315> (accessed on 1 October 2023).
35. Mohler, G.; Short, M.; Brantingham, P.; Schoenberg, F.; Tita, G. Self-Exciting Point Process Modeling of Crime. *J. Am. Stat. Assoc.* **2011**, *106*, 100–108. [\[CrossRef\]](#)
36. PredPol. The Science & Testing of Predictive Policing, The Predictive Policing Company. Available online: <https://cdn2.hubspot.net/hubfs/3362003/White%2520Paper%2520Science%2520&%2520Testing%2520of%2520Predictive%2520Policing.pdf> (accessed on 5 December 2023).
37. Eterno, J.A.; Silverman, E.B. The New York City police department’s Compstat: Dream or nightmare? *Int. J. Police Sci. Manag.* **2006**, *8*, 218–231. [\[CrossRef\]](#)
38. Azavea. HunchLab: Under the Hood. 2015. Available online: <https://blog.pilpul.me/files/2015/09/HunchLab-Under-the-Hood.pdf>, (accessed on 5 December 2023).
39. Barrett, L. Reasonably suspicious algorithms: Predictive policing at the United States border. *NYU Rev. L. Soc. Chang.* **2017**, *41*, 327.
40. Ferguson, A.G. Policing predictive policing. *Wash. U.L. Rev.* **2016**, *94*, 1109.
41. Saunders, J.; Hunt, P.; Hollywood, J.S. Predictions put into practice: A quasi-experimental evaluation of Chicago’s predictive policing pilot. *J. Exp. Criminol.* **2016**, *12*, 347–371. [\[CrossRef\]](#)
42. Hoggard, C. Fresno Police Scanning Social Media to Assess Threat. *abc30 Action News*. 2015. Available online: <https://abc30.com/fresno-police-social-media-big-brother-software/525999/> (accessed on 5 December 2023).
43. Robinson, D. Buyer Beware: A Hard Look at Police ‘Threat Scores’. 2016. Available online: <https://medium.com/equal-future/buyer-beware-a-hard-look-at-police-threat-scores-961f73b88b10/> (accessed on 5 December 2023).
44. Levine, E.S.; Tisch, J.; Tasso, A.; Joy, M. The New York City police department’s domain awareness system. *Interfaces* **2017**, *47*, 70–84. [\[CrossRef\]](#)
45. Saeed, U.; Sarim, M.; Usmani, A.; Mukhtar, A.; Shaikh, A.B.; Raffat, S.K. Application of machine learning algorithms in crime classification and classification rule mining. *Res. J. Recent Sci. ISSN* **2015**, *2277*, 2502.
46. Chen, H.; Schroeder, J.; Hauck, R.V.; Ridgeway, L.; Atabakhsh, H.; Gupta, H.; Boarman, C.; Rasmussen, K.; Clements, A.W. COPLINK Connect: Information and knowledge management for law enforcement. *Decis. Support Syst.* **2003**, *34*, 271–285. [\[CrossRef\]](#)
47. Egbert, S. Predictive policing and the platformization of police work. *Surveill. Soc.* **2019**, *17*, 83–88. [\[CrossRef\]](#)
48. De’ath, G.; Fabricius, K.E. Classification and regression trees: A powerful yet simple technique for ecological data analysis. *Ecology* **2000**, *81*, 3178–3192. [\[CrossRef\]](#)
49. Breiman, L. Random forests. *Mach. Learn.* **2001**, *45*, 5–32. [\[CrossRef\]](#)
50. Nath, S.V. Crime pattern detection using data mining. In Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops, Hong Kong, China, 18–22 December 2006; pp. 41–44.
51. Zhang, X.; Liu, L.; Xiao, L.; Ji, J. Comparison of machine learning algorithms for predicting crime hotspots. *IEEE Access* **2020**, *8*, 181302–181310. [\[CrossRef\]](#)

52. Safat, W.; Asghar, S.; Gillani, S.A. Empirical analysis for crime prediction and forecasting using machine learning and deep learning techniques. *IEEE Access* **2021**, *9*, 70080–70094. [\[CrossRef\]](#)
53. Chen, P.; Yuan, H.; Shu, X. Forecasting crime using the arima model. In Proceedings of the 2008 Fifth International Conference on Fuzzy Systems and Knowledge Discovery, Jinan, China, 18–20 October 2008; pp. 627–630.
54. Khan, J.R.; Saeed, M.; Siddiqui, F.A.; Mahmood, N.; Arifeen, Q.U. PREDICTIVE POLICING: A Machine Learning Approach to Predict and Control Crimes in Metropolitan Cities. *Univ. Sindh J. Inf. Commun. Technol.* **2019**, *3*, 17–26.
55. Babakura, A.; Sulaiman, M.N.; Yusuf, M.A. Improved method of classification algorithms for crime prediction. In Proceedings of the 2014 International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur, Malaysia, 26–27 August 2014; pp. 250–255.
56. Zhang, Q.; Yuan, P.; Zhou, Q.; Yang, Z. Mixed spatial-temporal characteristics based crime hot spots prediction. In Proceedings of the 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Nanchang, China, 4–6 May 2016; pp. 97–101.
57. Nitta, G.R.; Rao, B.Y.; Sravani, T.; Ramakrishiah, N.; Balaanand, M. LASSO-based feature selection and naïve Bayes classifier for crime prediction and its type. *Serv. Oriented Comput. Appl.* **2019**, *13*, 187–197. [\[CrossRef\]](#)
58. Shingleton, J.S. *Crime Trend Prediction Using Regression Models for Salinas, California*; Naval Postgraduate School: Monterey, CA, USA, 2012.
59. Wang, P.; Mathieu, R.; Ke, J.; Cai, H. Predicting criminal recidivism with support vector machine. In Proceedings of the 2010 International Conference on Management and Service Science, Wuhan, China, 24–26 August 2010; pp. 1–9.
60. Iqbal, R.; Murad, M.A.A.; Mustapha, A.; Panahy, P.H.S.; Khanahmadliravi, N. An Experimental Study of Classification Algorithms for Crime Prediction. *Indian J. Sci. Technol.* **2013**, *6*, 1–7. [\[CrossRef\]](#)
61. Ivan, N.; Ahishakiye, E.; Omulo, E.O.; Wario, R. A performance analysis of business intelligence techniques on crime prediction. *Int. J. Comput. Inf. Technol.* **2017**, *4*, 84–90.
62. Ahishakiye, E.; Taremwa, D.; Omulo, E.O.; Niyonzima, I. Crime prediction using decision tree (J48) classification algorithm. *Int. J. Comput. Inf. Technol.* **2017**, *6*, 188–195.
63. Aldossari, B.S.; Alqahtani, F.M.; Alshahrani, N.S.; Alhammam, M.M.; Alzamanan, R.M.; Aslam, N.; Irfanullah. A Comparative Study of Decision Tree and Naive Bayes Machine Learning Model for Crime Category Prediction in Chicago. In Proceedings of the 2020 6th International Conference on Computing and Data Engineering, Sanya, China, 4–6 January 2020; pp. 34–38.
64. Lin, Y.-L.; Chen, T.-Y.; Yu, L.-C. Using machine learning to assist crime prevention. In Proceedings of the 2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI), Hamamatsu, Japan, 9–13 July 2017; pp. 1029–1030.
65. McClendon, L.; Meghanathan, N. Using machine learning algorithms to analyze crime data. *Mach. Learn. Appl. Int. J. (MLAIJ)* **2015**, *2*, 1–12. [\[CrossRef\]](#)
66. Wheeler, A.P.; Steenbeek, W. Mapping the risk terrain for crime using machine learning. *J. Quant. Criminol.* **2021**, *37*, 445–480. [\[CrossRef\]](#)
67. Kang, H.-W.; Kang, H.-B. Prediction of crime occurrence from multi-modal data using deep learning. *PLoS ONE* **2017**, *12*, 176–244. [\[CrossRef\]](#)
68. Llahi, O. Crime analysis and prediction using machine learning. In Proceedings of the 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 28 September–2 October 2020; pp. 496–501.
69. Stec, A.; Klabjan, D. Forecasting crime with deep learning. *arXiv* **2018**, arXiv:1806.01486.
70. Almanie, T.; Mirza, R.; Lor, E. Crime prediction based on crime types and using spatial and temporal criminal hotspots. *arXiv* **2015**, arXiv:1508.02050. [\[CrossRef\]](#)
71. Zia, T.A.A.; Shehbaz, M.; Nawaz, M.S.; Shahzad, B.; Abdullatif, A.; Mustafa, R.; Lali, M.I. Identification of hatred speeches on Twitter. In Proceedings of the 52nd The IRES International Conference, Kuala Lumpur, Malaysia, 5–6 November 2016; pp. 27–32.
72. Gayathri, M.; Meghana, M.; Trivedi, M.; Manju, D. Suspicious Activity Detection and Tracking through Unmanned Aerial Vehicle Using Deep Learning Techniques. *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *9*, 2812–2816. [\[CrossRef\]](#)
73. Stalidis, P.; Semertzidis, T.; Daras, P. Examining deep learning architectures for crime classification and prediction. *Forecasting* **2021**, *3*, 46. [\[CrossRef\]](#)
74. Rajapakshe, C.; Balasooriya, S.; Dayarathna, H.; Ranaweera, N.; Walgampaya, N.; Pemadasa, N. Using cnns rnns and machine learning algorithms for real-time crime prediction. In Proceedings of the 2019 International Conference on Advancements in Computing (ICAC), Malabe, Sri Lanka, 5–7 December 2019; pp. 310–316.
75. Wang, B.; Yin, P.; Bertozzi, A.L.; Brantingham, P.J.; Osher, S.J.; Xin, J. Deep learning for real-time crime forecasting and its ternarization. *Chin. Ann. Math. Ser. B* **2019**, *40*, 949–966. [\[CrossRef\]](#)
76. Berk, R.A. Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annu. Rev. Criminol.* **2021**, *4*, 209–237. [\[CrossRef\]](#)
77. Singh, A.; Anand, T.; Sharma, S.; Singh, P. IoT based weapons detection system for surveillance and security using YOLOV4. In Proceedings of the 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 8–10 July 2021; pp. 488–493.
78. Velastin, S.A.; Boghossian, B.A.; Vicencio-Silva, M.A. A motion-based image processing system for detecting potentially dangerous situations in underground railway stations. *Transp. Res. Part C Emerg. Technol.* **2006**, *14*, 96–113. [\[CrossRef\]](#)

79. Bhatti, M.T.; Khan, M.G.; Aslam, M.; Fiaz, M.J. Weapon detection in real-time cctv videos using deep learning. *IEEE Access* **2021**, *9*, 34366–34382. [CrossRef]
80. Ahmed, S.; Bhatti, M.T.; Khan, M.G.; Löfström, B.; Shahid, M. Development and optimization of deep learning models for weapon detection in surveillance videos. *Appl. Sci.* **2022**, *12*, 5772. [CrossRef]
81. Kaya, V.; Tuncer, S.; Baran, A. Detection and classification of different weapon types using deep learning. *Appl. Sci.* **2021**, *11*, 7535. [CrossRef]
82. Ruiz-Santaquiteria, J.; Velasco-Mata, A.; Vallez, N.; Bueno, G.; Alvarez-Garcia, J.A.; Deniz, O. Handgun detection using combined human pose and weapon appearance. *IEEE Access* **2021**, *9*, 123815–123826. [CrossRef]
83. Hashmi, T.S.S.; Haq, N.U.; Fraz, M.M.; Shahzad, M. Application of deep learning for weapons detection in surveillance videos. In Proceedings of the 2021 International Conference on Digital Futures and Transformative Technologies (ICoDT2), Islamabad, Pakistan, 20–21 May 2021; pp. 1–6.
84. Narejo, S.; Pandey, B.; Esenarro Vargas, D.; Rodriguez, C.; Anjum, M.R. Weapon detection using YOLO V3 for smart surveillance system. *Math. Probl. Eng.* **2021**, *2021*, 9975700. [CrossRef]
85. Verma, G.K.; Dhillon, A. A handheld gun detection using faster r-cnn deep learning. In Proceedings of the 7th International Conference on Computer and Communication Technology, Nagpur, India, 11–13 November 2017; pp. 84–88.
86. Ingle, P.Y.; Kim, Y.-G. Real-time abnormal object detection for video surveillance in smart cities. *Sensors* **2022**, *22*, 3862. [CrossRef] [PubMed]
87. Velasco-Mata, A.; Ruiz-Santaquiteria, J.; Vallez, N.; Deniz, O. Using human pose information for handgun detection. *Neural Comput. Appl.* **2021**, *33*, 17273–17286. [CrossRef]
88. Simonyan, K.; Zisserman, A. Very deep convolutional networks for large-scale image recognition In: Proceedings of International Conference on Learning Representations. *arXiv* **2015**, arXiv:1409.1556.
89. Redmon, J.; Divvala, S.; Girshick, R.; Farhadi, A. You only look once: Unified, real-time object detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 27–30 June 2016; pp. 779–788.
90. Redmon, J.; Farhadi, A. YOLO9000: Better, faster, stronger. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Honolulu, HI, USA, 21–26 July 2017; pp. 7263–7271.
91. Redmon, J.; Farhadi, A. Yolov3: An incremental improvement. *arXiv* **2018**, arXiv:1804.02767.
92. Bochkovskiy, A.; Wang, C.-Y.; Liao, H.-Y.M. Yolov4: Optimal speed and accuracy of object detection. *arXiv* **2020**, arXiv:2004.10934.
93. Sajjad, M.; Nasir, M.; Muhammad, K.; Khan, S.; Jan, Z.; Sangaiah, A.K.; Elhoseny, M.; Baik, S.W. Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. *Future Gener. Comput. Syst.* **2020**, *108*, 995–1007. [CrossRef]
94. Sermanet, P.; Eigen, D.; Zhang, X.; Mathieu, M.; Fergus, R.; LeCun, Y. Overfeat: Integrated recognition, localization and detection using convolutional networks. *arXiv* **2013**, arXiv:1312.6229.
95. Zhang, H.; Berg, A.C.; Maire, M.; Malik, J. SVM-KNN: Discriminative nearest neighbor classification for visual category recognition. In Proceedings of the 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06), New York, NY, USA, 17–22 June 2006; pp. 2126–2136.
96. County of Los Angeles Enterprise GIS. Available online: <https://egis-lacounty.hub.arcgis.com/> (accessed on 27 September 2023).
97. Chicago Data Portal. Available online: <https://data.cityofchicago.org/stories/s/5cd6-ry5g> (accessed on 26 September 2023).
98. Communities and Crime. Available online: <https://archive.ics.uci.edu/dataset/183/communities+and+crime> (accessed on 27 September 2023).
99. Chicago Crime. Available online: <https://www.kaggle.com/datasets/chicago/chicago-crime> (accessed on 26 September 2023).
100. Mississippi Crime Rates and Statistics—NeighborhoodScout. Available online: <https://www.neighborhoodscout.com/ms/crime> (accessed on 27 September 2023).
101. City of Dallas Open Data. Available online: <https://www.dallasopendata.com/> (accessed on 27 September 2023).
102. Weather Underground. Available online: <https://www.wunderground.com/> (accessed on 27 September 2023).
103. Google. Google Street View. Available online: <https://developers.google.com/maps/documentation/streetview/> (accessed on 27 September 2023).
104. Data.denvergov.org. Denver Open Data Catalog: Crime. Available online: <https://denvergov.org/opendata> (accessed on 27 September 2023).
105. US City Open Data Census—Datasets. Available online: <https://us-cities.survey.okfn.org/> (accessed on 27 September 2023).
106. Dixon, A.; Birks, D. Improving policing with natural language processing. In Proceedings of the 1st Workshop on NLP for Positive Impact, Online, 5 August 2021; pp. 115–124.
107. Chowdhary, K.; Chowdhary, K.R. Natural language processing. *Fundam. Artif. Intell.* **2020**, 603–649.
108. Campedelli, G.M. Where are we? Using Scopus to map the literature at the intersection between artificial intelligence and research on crime. *J. Comput. Soc. Sci.* **2021**, *4*, 503–530. [CrossRef]
109. Birks, D.; Coleman, A.; Jackson, D. Unsupervised identification of crime problems from police free-text data. *Crime Sci.* **2020**, *9*, 18. [CrossRef]
110. Kuang, D.; Brantingham, P.J.; Bertozzi, A.L. Crime topic modeling. *Crime Sci.* **2017**, *6*, 12. [CrossRef]
111. Basilio, M.P.; Brum, G.S.; Pereira, V. A model of policing strategy choice: The integration of the Latent Dirichlet Allocation (LDA) method with ELECTRE I. *J. Model. Manag.* **2020**, *15*, 849–891. [CrossRef]

112. Basilio, M.P.; Pereira, V.; Brum, G. Identification of operational demand in law enforcement agencies: An application based on a probabilistic model of topics. *Data Technol. Appl.* **2019**, *53*, 333–372. [\[CrossRef\]](#)
113. Karystianis, G.; Adily, A.; Schofield, P.; Knight, L.; Galdon, C.; Greenberg, D.; Jorm, L.; Nenadic, G.; Butler, T. Automatic extraction of mental health disorders from domestic violence police narratives: Text mining study. *J. Med. Internet Res.* **2018**, *20*, e11548. [\[CrossRef\]](#)
114. Karystianis, G.; Adily, A.; Schofield, P.W.; Greenberg, D.; Jorm, L.; Nenadic, G.; Butler, T. Automated analysis of domestic violence police reports to explore abuse types and victim injuries: Text mining study. *J. Med. Internet Res.* **2019**, *21*, e13067. [\[CrossRef\]](#) [\[PubMed\]](#)
115. Almeahmadi, A.; Joudaki, Z.; Jalali, R. Language usage on Twitter predicts crime rates. In Proceedings of the 10th International Conference on Security of Information and Networks 2017, Hong Kong, China, 29 November–2 December 2017; pp. 307–310.
116. Wang, X.; Gerber, M.S.; Brown, D.E. Automatic crime prediction using events extracted from twitter posts. In *International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 231–238.
117. Chau, M.; Xu, J.J.; Chen, H. Extracting meaningful entities from police narrative reports. In the UA Campus Libraries at The University of Arizona. 2002. Available online: <http://hdl.handle.net/10150/105786/> (accessed on 5 December 2023).
118. Carnaz, G.; Beires Nogueira, V.; Antunes, M.; Ferreira, N. An automated system for criminal police reports analysis. In *Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018) 10*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; pp. 360–369. [\[CrossRef\]](#)
119. Arulanandam, R.; Savarimuthu, B.T.R.; Purvis, M. Extracting crime information from online newspaper articles. In Proceedings of the Second Australasian Web Conference, Auckland, New Zealand, 20–23 January 2014; pp. 31–38.
120. Shabat, H.A.; Omar, N. Named entity recognition in crime news documents using classifiers combination. *Middle-East J. Sci. Res.* **2015**, *23*, 1215–1221.
121. Yang, Y.; Manoharan, M.; Barber, K.S. Modelling and analysis of identity threat behaviors through text mining of identity theft stories. In Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference, The Hague, The Netherlands, 24–26 September 2014; pp. 184–191.
122. Schraagen, M.; Brinkhuis, M.; Bex, F. Evaluation of Named Entity Recognition in Dutch online criminal complaints. *Comput. Linguist. Neth. J.* **2017**, *7*, 3–16.
123. Al-Zaidy, R.; Fung, B.C.; Youssef, A.M. Towards discovering criminal communities from textual data. In Proceedings of the 2011 ACM Symposium on Applied Computing, TaiChung, Taiwan, 21–24 March 2011; pp. 172–177.
124. Pinheiro, V.; Furtado, V.; Pequeno, T.; Nogueira, D. Natural language processing based on semantic inferentialism for extracting crime information from text. In Proceedings of the IEEE International Conference on Intelligence and Security Informatics, Vancouver, BC, Canada, 23–26 May 2010; pp. 19–24.
125. Yang, K.-S.; Chen, C.-C.; Tseng, Y.-H.; Ho, Z.-P. Name entity extraction based on POS tagging for criminal information analysis and relation visualization. In Proceedings of the 6th International Conference on New Trends in Information Science, Service Science and Data Mining (ISSDM2012), Taipei, Taiwan, 23–25 October 2012; pp. 785–789.
126. Asharef, M.; Omar, N.; Albared, M.; Minhui, Z.; Weiming, W.; Jingjing, Z. Arabic named entity recognition in crime documents. *J. Theor. Appl. Inf. Technol.* **2012**, *44*, 1–6.
127. Alkaff, A.; Mohd, M. Extraction of Nationality from Crime News. *J. Theor. Appl. Inf. Technol.* **2013**, *54*, 304–312.
128. Pandey, S.; Jain, N.; Bhardwaj, A.; Kaur, G. Leveraging Machine Learning and Natural Language Processing for Predicting the Crime Rate: Reach 360. In Proceedings of the 3rd International Conference on Internet of Things and Connected Technologies (ICIOTCT), Jaipur, India, 26–27 March 2018; pp. 26–27.
129. Saraiva, M.; Matijosaitiene, I.; Mishra, S.; Amante, A. Crime prediction and monitoring in porto, portugal, using machine learning, spatial and text analytics. *ISPRS Int. J. Geo-Inf.* **2022**, *11*, 400. [\[CrossRef\]](#)
130. Han, S.; Huang, H.; Liu, J.; Xiao, S. American hate crime trends prediction with event extraction. *arXiv* **2021**, arXiv:2111.04951.
131. Ozalp, S.; Williams, M.L.; Burnap, P.; Liu, H.; Mostafa, M. Antisemitism on Twitter: Collective efficacy and the role of community organisations in challenging online hate speech. *Soc. Media + Soc.* **2020**, *6*, 2056305120916850. [\[CrossRef\]](#)
132. Pereira-Kohatsu, J.C.; Quijano-Sánchez, L.; Liberatore, F.; Camacho-Collados, M. Detecting and monitoring hate speech in Twitter. *Sensors* **2019**, *19*, 4654. [\[CrossRef\]](#)
133. Ku, C.H.; Iriberry, A.; Leroy, G. Crime information extraction from police and witness narrative reports. In Proceedings of the IEEE Conference on Technologies for Homeland Security, Waltham, MA, USA, 12–13 May 2008; pp. 193–198.
134. Ku, C.H.; Iriberry, A.; Leroy, G. Natural language processing and e-government: Crime information extraction from heterogeneous data sources. In Proceedings of the 2008 International Conference on Digital Government Research, Melbourne, Australia, 23–24 October 2008; pp. 162–170.
135. Anderson, N.; Belavy, D.L.; Perle, S.M.; Hendricks, S.; Hespanhol, L.; Verhagen, E.; Memon, A.R. AI did not write this manuscript, or did it? Can we trick the AI text detector into generated texts? The potential future of ChatGPT and AI in Sports & Exercise Medicine manuscript generation. *BMJ Open Sport Exerc. Med.* **2023**, *9*, e001568. [\[PubMed\]](#)
136. Hayward, K.J.; Maas, M.M. Artificial intelligence and crime: A primer for criminologists. *Crime Media Cult.* **2021**, *17*, 209–233. [\[CrossRef\]](#)

137. Cooke, D.J.; Michie, C. Violence risk assessment: From prediction to understanding—Or from what? To why? In *Managing Clinical Risk*; Routledge: Oxford, UK, 2012; pp. 3–25.
138. Oswald, M.; Grace, J.; Urwin, S.; Barnes, G.C. Algorithmic risk assessment policing models: Lessons from the Durham HART model and ‘Experimental’ proportionality. *Inf. Commun. Technol. Law* **2018**, *27*, 223–250. [CrossRef]
139. Babuta, A.; Oswald, M.; Rinik, C. Machine Learning Algorithms and Police Decision-Making: LEGAL, Ethical and Regulatory Challenges. 2018. Available online: <https://nrl.northumbria.ac.uk/id/eprint/40579/> (accessed on 5 December 2023).
140. Babuta, A.; Oswald, M. Machine Learning Predictive Algorithms and the Policing of Future Crimes: Governance and Oversight. Available online: <https://ssrn.com/abstract=3479081> (accessed on 1 October 2023).
141. Mittelstadt, B. Automation, algorithms, and politics | auditing for transparency in content personalization systems. *Int. J. Commun.* **2016**, *10*, 12.
142. Alikhademi, K.; Drobin, E.; Prioleau, D.; Richardson, B.; Purves, D.; Gilbert, J.E. A review of predictive policing from the perspective of fairness. *Artif. Intell. Law* **2022**, *30*, 1–17. [CrossRef]
143. Joh, E.E. Feeding the Machine: Policing, Crime Data, & Algorithms. *William Mary Bill Rights J.* **2017**, *26*, 287.
144. Goldenfein, J. *Algorithmic Transparency and Decision-Making Accountability: Thoughts for Buying Machine Learning Algorithms*; Office of the Victorian Information Commissioner: Melbourne, Australia, 2019; Closer to the Machine: Technical, Social, and Legal Aspects of AI; Available online: <https://ssrn.com/abstract=3445873> (accessed on 1 October 2023).
145. Blodgett, S.L.; Barocas, S.; Daume III, H.; Wallach, H. Language (technology) is power: A critical survey of “bias” in nlp. *arXiv* **2020**, arXiv:2005.14050.
146. Lum, K.; Isaac, W. Predictive policing reinforces police bias. *Hum. Rights Data Anal. Group* **2016**, *10*.
147. Kusner, M.J.; Loftus, J.; Russell, C.; Silva, R. Counterfactual Fairness. In Proceedings of the Advances in Neural Information Processing Systems, Long Beach, CA, USA, 4–9 December 2017; pp. 4066–4076.
148. Dwork, C.; Hardt, M.; Pitassi, T.; Reingold, O.; Zemel, R. Fairness through awareness. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference 2012, Cambridge, MA, USA, 8–10 January 2012; pp. 214–226.
149. Corbett-Davies, S.; Pierson, E.; Feller, A.; Goel, S.; Huq, A. Algorithmic decision making and the cost of fairness. In Proceedings of the 23rd Acm Sigkdd International Conference on Knowledge Discovery and Data Mining, Halifax, NS, Canada, 13–17 August 2017; pp. 797–806.
150. Hardt, M.; Price, E.; Srebro, N. Equality of opportunity in supervised learning. *arXiv* **2016**, arXiv:1610.02413.
151. Grgic-Hlaca, N.; Zafar, M.B.; Gummadi, K.P.; Weller, A. The case for process fairness in learning: Feature selection for fair decision making. *NIPS Symp. Mach. Learn. Law* **2016**, *1*, 11.
152. Verma, S.; Rubin, J. Fairness Definitions Explained. In Proceedings of the International Workshop on Software Fairness, Gothenburg, Sweden, 29 May 2018; pp. 1–7.
153. Asaro, P.M. AI ethics in predictive policing: From models of threat to an ethics of care. *IEEE Technol. Soc. Mag.* **2019**, *38*, 40–53. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.