Accountable Predictive Policing of Cybercrime? Insights from Nigerian Law Enforcement

IE Nwafor*

Online ISSN
1727-3781

P·E·R
Pioneer in peer-reviewed, open access online law publications

Author

Ifeoma Nwafor

Affiliation

Godfrey Okoye University, Nigeria

Email

ifeomanwafor900@gmail.com

Date Submitted

9 September 2025

Date Revised

14 May 2026

Date Accepted

14 May 2026

Date Published

21 July 2026

Guest editors

Prof Chijioke Okorie
Prof Vukosi Marivate

Journal Editor

Prof Wian Erlank

How to cite this contribution

Nwafor IE "Accountable Predictive Policing of Cybercrime? Insights from Nigerian Law Enforcement" *PER / PELJ* 2026(29) - DOI http://dx.doi.org/10.17159/1727-3781/2026/v29i0a23879

Copyright

DOI
http://dx.doi.org/10.17159/1727-3781/2026/v29i0a23879

Abstract

The unconventional challenges in cybercrime investigation and mitigation brought about by the sophistication of artificial intelligence (AI) significantly affect the fight against cybercrime. Cybercriminals employ AI and machine learning to bypass cybersecurity defences and expand the scope of cyber threats. There is an ongoing debate about how AI can enable defenders to detect, predict and effectively respond to cyber threats using technologies such as predictive policing tools. However, the effectiveness of predictive policing has not been widely accepted in contemporary scientific literature due to the human rights, legal and ethical concerns that inhibit its use in cybercrime mitigation. A remarkable quantity of cybercrime is perpetrated by Nigerians globally and in Nigeria, compared with other countries. Nigeria ranks fifth globally as a source of cybercrime and cybercriminal activity, according to the world's first Cybercrime Index. Nigeria also ranks thirteenth on the Global Threat Index amongst the countries most vulnerable to cyberattacks. Nigerian law enforcement agencies are ill-equipped to confront the technological advancements in cybercrime. This study, based on qualitative and desktop research, explores the necessary adaptation of existing predictive policing techniques to the Nigerian cybercrime situation, taking into account the problematisation of what predictive policing represents today. It conducts a criminological analysis of the law enforcement response to cybercrime in Nigeria, highlighting the role of digitalisation in cybercrime prevention. Additionally, it examines the legal status of predictive policing technologies in Nigeria, including their compliance and risk management considerations. Based on insights from Nigerian law enforcement, this study found that predictive policing is not a preventive measure for combating cybercrime in Nigeria due to the legal, ethical and human rights concerns inherent in such AI-driven tools across all domains of their use. It is found that the legal status of predictive policing systems in Nigeria remains ambiguous, as there is no dedicated AI governance and regulatory framework governing their legal position and use. Additionally, the formal measurement or oversight of compliance and risk management regarding predictive policing deployment in Nigerian law enforcement is limited and largely *ad hoc* due to the absence of specific AI regulation in Nigeria.

Keywords

Artificial intelligence; AI; cybercrime; predictive policing; predictive policing of cybercrime; algorithmic accountability; AI ethics; AI in criminal justice; crime pattern identification; cybercrime forecasting.

.....

1 Introduction

Cybercriminals consistently outpace law enforcement by exploiting online security vulnerabilities and emerging technologies to intensify cybercrime, resulting in billions of dollars in losses across multiple countries.[1] The 2023 African Cybersecurity Assessment Report[2] highlights online scams, cyber extortion, business e-mail compromise, phishing, ransomware attacks, banking trojans and stealers, and crimeware-as-a-service as prominent cyber threats in Africa. Nigeria ranks fifth globally as a source of cybercrime and cybercriminal activity according to the Cybercrime Index, which maps the global geography of cybercrime.[3] The ranking of the countries highlighted for high cybercriminal activity was based on the impact, professionalism, and technical skill of their offenders. Additionally, Nigeria is ranked the thirteenth most vulnerable country to cyberattacks on the Global Threat Index. Nigeria moved from the 35th to the 13th place within seven years, highlighting the fact that there is a troubling increase in cybercrime.[4]

There is an ongoing debate about the efficacy of predictive policing and its role in mitigating cybercrime. Several nations have explored the use of predictive policing algorithms to forecast criminal activities. Its effectiveness is far from being universally accepted in scientific and contemporary literature, owing to issues relating to racial bias, accountability,

* Ifeoma E Nwafor. LLB LLM PhD. Faculty of Law, Godfrey Okoye University, Nigeria. E-mail: nwaforifeoma@gouni.edu.ng. Adjunct Professor, Lincoln Alexander School of Law, Toronto Metropolitan University, Canada. E-mail: ifeoma.nwafor@torontomu.ca. The research for the work in this article received ethical approval from Godfrey Okoye University's Research Ethics Committee under Ethical Clearance Nos. GOU/R/HR/DE/0612/2023. A portion of this article was presented at the Third African Forum on Cybercrime and Electronic Evidence organised by the Council of Europe, the European Union and the Kenyan Government in November 2025 in Nairobi, Kenya. The work is based on research supported in part by the Coimbra Group during my research stay at the Faculty of Law and Criminology, KU Leuven, Belgium. It forms part of the Legal–Technical AI Governance in Africa project hosted by the Data Science Law Lab at the University of Pretoria. The work was supported in part by funding provided to the University of Pretoria through a gift from Meta. The views and opinions expressed in this publication are those of the author(s) and do not necessarily reflect those of the University of Pretoria, Meta, or affiliated institutions. I extend my sincere gratitude to Professor Peggy Valcke, my academic host as a visiting scholar at the Faculty of Law and Criminology, KU Leuven, Belgium, for providing invaluable guidance and resources. ORCiD: https://orcid.org/ 0000-0001-9288-2378.

1 Interpol 2023 https://cybilportal.org/publications/african-cyberthreat-assessment-report-2023-cyberthreat-trends/.

2 The survey was conducted by the African Cybercrime Operations Desk and the data were drawn from Interpol's member countries.

3 Bruce *et al* 2024 *PLoS ONE* 8.

4 Check Point Software Technologies 2025 *African Perspectives on Cyber Security Report 2025* https://www.securitysa.com/ex/AfricanSecurityReport_2025.pdf accessed 10 May 2026.

transparency, governance and privacy concerns, among others. Studies on the development of techniques for detecting and preventing cybercrime have been conducted.[5] Cybercrime detection models have been proposed for cyberbullying,[6] fake news,[7] and denial-of-service/distributed denial-of-service attacks.[8] Amer, Siddiqui and Athamena have proposed a cybercriminal detection model using neural networks, deep learning and machine learning to detect cyberbullying.[9] A study of crime prediction in Poland,[10] Germany[11] and Belgium[12] has been conducted. Kosinski and Krasnodebski relied on police statistical data on cybercrime in Poland between 2002 and 2019 to predict cybercrime in Poland for the year 2020. The survey found that global cybercrime predictions, particularly regarding copyright infringement/related rights, counterfeiting/computer fraud and crimes against confidentiality, integrity and availability are inaccurate because the amounts of cybercrime vary across these categories. The authors expressed the opinion that cybercrime prediction is much more accurate when conducted in terms of the detection rate, as the quality of law enforcement preparedness determines the level, and this factor does not change randomly.[13]

The impact of AI models in matching emerging technologies-enabled cybercrime,[14] the ethical challenges of data-driven policing,[15] and the drawbacks of profiling and prediction in cybercrime research datafication have been accorded attention.[16] The literature on predictive policing focuses on its adverse effects and the need for reform.[17] There is existing literature on the impacts and drawbacks of AI models for cybercrime detection and prevention,[18] and proposals for and predictions of the development of such models,[19] but there is a gap in the existing literature: the question of whether cybercrime practices can be prevented/combatted by the concrete predictive policing strategies of the Nigerian law enforcement is underexplored. This study fills this gap by exploring the

5 Mulahuwaish *et al* 2025 *Computers in Human Behavior Reports*.
6 Sultan *et al* 2022 *Computers, Materials & Continua;* Raj *et al* 2021 *Electronics*; Pericherla and Ilavarasan 2024 *International Journal of Intelligent Unmanned Systems*.
7 Fouad, Sabbeh and Medhat 2022 *Computers, Materials & Continua* 3647.
8 Khan *et al* 2021 https://doi.org/10.21203/rs.3.rs-271920/v1.
9 Amer, Siddiqui and Athamena 2022 https://doi.org/10.21203/rs.3.rs-2184218/v1.
10 Kosiński and Krasnodebski "Crime Predicting in the Light of Police Statistics".
11 Egbert 2018 *European Journal of Security Research*.
12 Antonov *et al Predictive Policing*.
13 Kosiński and Krasnodebski "Crime Predicting in the Light of Police Statistics" 64.
14 Treleaven *et al* 2023 https://dx.doi.org/10.2139/ssrn.4507244.
15 Davis *et al* 2022 *AI and Ethics* 185-188.
16 Custers "Profiling and Predictions".
17 Hobson *et al* 2023 *Journal of Experimental Criminology* 165.
18 Mulahuwaish *et al* 2025 *Computers in Human Behavior Reports*.
19 Mulahuwaish *et al* 2025 *Computers in Human Behavior Reports*.

transposition of predictive policing models to fight cybercrime in Nigeria, bearing in mind the problematisation of what predictive policing represents nowadays. It conducts a criminological analysis of Nigeria's current capacity to respond to cybercrime, the reactions of Nigerian law enforcement agencies to cybercrime, and the role of digitalisation in mitigating cybercrime in Nigeria.

Additionally, it examines the legal status of predictive policing technologies in Nigeria, including their compliance and risk management. The article discusses the AI regulatory landscape in Nigeria, including the Nigerian *Data Protection Act*, 2023, and the Nigerian *Cybercrime Act*, 2024, which is Nigeria's cyber-specific legislation. There is an evolving intersection between AI and cybercrime, and cybercriminals are leveraging advanced technologies to escalate various cybercrime activities. Reviewing the Nigerian cybercrime legislation is justified to ensure that it addresses AI-driven cyber-attacks and maintains technological neutrality. The survey reveals that Nigerian law enforcement agencies are not fully equipped to respond to cybercrime. Cybercrime regulators in Nigeria believe that although there are patterns in cybercriminal behaviour that make predictive policing a valuable tool for combating cybercrime, critical concerns about such tools undermine their preventive capacity. It is also found that the legal status of predictive policing systems in Nigeria remains ambiguous, as there is no AI governance and regulatory framework governing their legal position and use.

The technical and criminological findings of the study will strengthen AI governance in Nigeria and significantly contribute to the transdisciplinary discourse. Following this introduction, the article consists of four parts. Part Two provides contextual grounding and offers an overview of predictive policing, including its current practice, its application to cybercrime, and its potential benefits and risks. Part Three examines the existing laws relevant to predictive policing and cybercrime in Nigeria, and Part Four provides concluding remarks.

1.1 Methodology

This is primarily a qualitative study conducted through the administration of a questionnaire to sixteen subjects and five in-depth, structured interviews with law enforcement agents from the Cybercrime Units of the Nigerian Economic and Financial Crimes Commission (EFCC) across all geopolitical regions in Nigeria. The participants included members and heads of the Commission's cybercrime units, who provided informed consent and understood the nature of the research. The questionnaire contained 25 questions. The interviews and survey were conducted online between July 2024 and May 2025. The EFCC is a central cybercrime regulatory agency

in Nigeria particularly focused on financial cybercrime.[20] Section 6 of the *Economic and Financial Crimes Commission (Establishment) Act*, 2004 (*EFCC Act*) gives the Commission the responsibility to investigate all financial crimes, including advance fee fraud, computer crime, money laundering, and fraudulent encashment.[21]

Ethical clearance for this research was obtained from the Directorate of Ethics at Godfrey Okoye University, Nigeria, and the terms of the approval were duly complied with. The consent of the participants in the research was duly obtained. The participants were selected with the assistance of the Department of Planning, Policy, Research and Statistics of the EFCC.

The criminological analysis aimed to gain qualitative insight into law enforcement agents' opinions of Nigeria's readiness, the role of digitalisation, and the use of predictive policing models in combatting cybercrime in Nigeria. The goal of the study was to determine Nigeria's cybercrime detection rate, law enforcement agents' understanding of AI policing tools, the feasibility of translating such tools into combatting cybercrime in Nigeria, and the legal status of AI technologies in Nigeria. The technical and criminological findings of the study will strengthen AI governance in Nigeria, influencing the ability of the framework to meet objectives, operate ethically, and manage risk and compliance effectively.

1.2 Criminological analysis findings

Approximately 14.2% of the responses highlighted that Nigeria's ability to respond to cybercrime is high. 35.7% of respondents stated that they believe the response to cybercrime is average and needs more work, and 14.2% believe little to no effort is being made. 80% of survey participants stated that AI-driven cybercrime makes investigations challenging. 73.3% expressed the belief that there are cybercrime patterns that make predictive policing suitable to mitigate cybercrime in Nigeria. However, 74% of the participants were unaware of the ethical challenges surrounding AI. This indicates a readiness and capacity gap. Nigerian law enforcement lacks the technological infrastructure and know-how to combat AI-based cybercrime, and a comprehensive cybercrime database. Many cybercrimes remain unreported, resulting in incomplete datasets for AI training. The data drawn from the in-depth interview shows that the legal standing and compliance

20 The EFCC is not the sole cybercrime regulatory agency in Nigeria. Other specialised bodies include the Cybercrime Prosecution Unit in the Attorney General's Office and the Specialised Police Cybercrime Unit within the Nigeria Police Force.

21 *Economic and Financial Crimes Commission (Establishment) Act*, 2004 (*EFCC Act*). See ss 6(6), 7 and 46. The powers of the Commission are further widened by ss 7(1)(a), 7(2)(f) and 13(2), which give it the powers to investigate and prosecute offenders for any offence, whether under the *EFFC Act* or any other statute. The underlying requirement is that the offence relates to the commission of economic and financial crimes. Most cybercrimes are related to financial crimes.

management of such policing cannot be ascertained due to the absence of an AI legal or regulatory framework in Nigeria.

1.3 Cybercrime in Nigeria

The growth of cybercrime in Nigeria has been alarming. It is difficult to determine with exactitude when the first act of cybercrime occurred in Nigeria.[22] However, there are noteworthy milestones in the history of cybercrime in Nigeria. Between 1995 and 1998 some Nigerians, namely Emmanuel Nwude, Ikechukwu Anajemba and Amaka Anajemba collaborated with some Asians involved in a financial crime that was dubbed the largest scam of its kind in Nigeria and the third-largest private scam in documented history.[23] The perpetrators defrauded and looted Nelson Sakaguchi and Branco Noroeste, Brazil's largest bank, of $224 million, leading to the bank's liquidation.[24] In 2020, the United Arab Emirates investigators arrested Ramon Olorunwa Abbas, known as Ray Hushpuppi, a Nigerian national, and handed him over to FBI agents. Federal prosecutors alleged that Hushpuppi had led a global network that had defrauded companies of hundreds of millions of dollars through business email compromise schemes, computer intrusion and money laundering.[25] In 2022 he was sentenced to eleven years in a US prison for money laundering.

In May 2022 three Nigerians were arrested by Interpol for allegedly engaging in global scamming. This arrest followed the publication of the Interpol Cyber Report, which links a suspected syndicate of Nigerian fraudsters to a malicious Remote Access Trojan (RAT) known as Agent Tesla, which reroutes financial transactions and steals confidential online connection details from corporate and regional organisations.[26] In 2024, the EFCC arrested seventeen people allegedly involved in a cyber fraud ring.[27]

---

22 This is because of the dearth of information gathering about cybercrime. Also, there have been dissenting views on what conducts amounts to cybercrime in the past.

23 Akande 2024 https://www.pulse.ng/story/emmanuel-nwude-sold-an-imaginary-airport-for-dollar242-million-2024080104383789077.

24 Nwude and Ikechukwu Anajemba impersonated the CBN Governor and the CBN's Director of International Remittance, respectively. With the use of false correspondence and high-level documents, they were able to convince Sakaguchi that the Nigerian government was seeking investors to build an airport in Abuja. The deal was that if Sakaguchi could provide the first investment, which was the sum of $242 million dollars, he would be entitled to 10% of that amount.

25 Mathers 2020 https://www.independent.co.uk/news/world/middle-east/huspuppi-instagram-news-arrested-cyberscam-350-million-a9590826.html.

26 Daniel 2022 https://www.vanguardngr.com/2022/05/interpol-4/.

27 Alagic-Bowder 2022 https://www.occrp.org/en/news/nigeria-arrests-17-cybercrime-suspects.

Two Nigerian brothers were convicted for sextortion targeting teenagers, which eventually led to the suicide of the victim, Jordan DeMay.[28]

The Nigerian cyber threat landscape is fuelled by several factors, including an increased poverty rate, unemployment, interconnectedness, internet accessibility, a misguided value system, inadequate educational systems, and limited opportunities in the workplace, at home and in the cloud.[29] It is essential to recognise that cybercrime cannot be equated to any interpersonal property offence and cannot be justified by individual economic determinants, like random theft. Cybercrime integrates into webs of financial and government activities. Several past Nigerian governors have been arrested and successfully prosecuted for money laundering.[30] Some government officials at the state and federal levels integrate stolen government funds into legitimate financial channels, a practice known as money laundering.

The preceding contextualisation of the Nigerian case study provides a picture of the magnitude of cybercrime in Nigeria, which is a very concerning phenomenon. The high rate of cybercrime perpetrated by Nigerians globally and in Nigeria is alarming. Cybercriminals employ AI and machine learning (ML) to penetrate cybersecurity defences set up by organisations and individuals.[31] It is essential to explore these policing tools to determine if and how they can assist in cybercrime detection and prevention. The following section provides contextual grounding in predictive policing systems and their application to cybercrimes, offering insight into the concept of predictive policing.

2 Overview of predictive policing

The employment of internet technology (IT) to enhance policing dates back about 25 years.[32] There is no unanimous definition of predictive policing in the existing literature, but there is some consensus on its crucial characteristics.[33] Egbert and Leese defines it as "the proactive use of algorithmically mediated data analysis to find patterns in datasets, based on which risk estimates are produced for prevention measures".[34] Udo notes that "Algorithmic or predictive policing (AP) typically applies third-party tree-based risk training algorithms (e.g. PredPol, HunchLab, Plantir) on criminal

28 Tidy 2024 https://www.bbc.com/news/articles/cr7rxpdyz9yo.
29 Okpe and Taya 2018 *Asian Journal of Multidisciplinary Studies* 1-12.
30 Nwafor 2022 *OAU Law Journal* 1-18.
31 Deloitte 2022 https://www.deloitte.com/content/dam/assets-zone1/gh/en/docs/services/risk-advisory/2023/Nigeria-Cybersecurity-Outlook-2022.pdf.
32 Mastrobuoni 2020 *Review of Economic Studies* 2735.
33 Meijer and Wessels 2019 *International Journal of Public Administration*.
34 Egbert and Leese *Criminal Future* 19.

complaint data to predict where and when the next crime is likely to occur, and who the likeliest perpetrators are. This way, AP pre-emptively determines where, how and when to deploy police resources."[35] One of the significant characteristics of predictive policing is that it uses vast quantities of data from numerous databases, algorithms, and swift computer processing to identify patterns or correlations that humans often ignore, thereby classifying new instances in the area of interest.[36] Its main objective is to further an empirical turn in police efforts, so that police decisions are based on technologically enhanced, objectively driven analytics rather than human subjectivity and bias.[37]

The preceding definitions suggest that predictive policing aims to aid law enforcement in preventing future crimes by analysing past crime patterns. This prediction examines trends and occurrences of crime to forecast crime hotspots and likely offenders and victims, and to channel police resources towards the predicted future crime. Predictive policing can be likened to forecasting the place, offender or victim of future crime.

2.1 How predictive policing works

Most predictive policing models involve rule-based machine learning. Law enforcement teaches AI systems which responses work best to predict cyberattacks.[38] Predictive policing by law enforcement agencies incorporates Big Data analytics tools to identify and prevent incidents.[39] Machine learning uses historical data[40] and statistical analysis to recognise and learn cybercrime patterns, enabling the detection of potential cybercrimes.[41] Three types of machine learning used in cybercrime detection are supervised learning, unsupervised learning and reinforcement learning. Predictive policing models cluster and forensically analyse data to identify past cyberattack methods and match them with billions of new data points, thereby predicting future cyber threats.[42] Thus, when an attack occurs, the system can provide appropriate recommendations to assist with risk management. It is important to note that the quality and accuracy of a machine learning model depend on the quality of the input data and the

35 Udoh "Is the Data Fair?" 1.
36 Davis *et al* 2022 *AI and Ethics* 193.
37 Davis *et al* 2022 *AI and Ethics* 193-195.
38 Storbeck 2022 https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf 13.
39 Schlehahn *et al* "Benefits and Pitfalls of Predictive Policing" 145.
40 Historical data are transferred to systems that use algorithms to create machine learning models that continuously train the systems to increase accuracy.
41 Gottsegen 2023 https://builtin.com/artificial-intelligence/machine-learning-cybersecurity.
42 Simon 2025 https://www.ibm.com/new/product-blog/ai-powered-threat-intelligence-predicting-cyber-attacks-before-they-happen.

algorithm's alignment with the use case.[43] This means that if the input data does not capture the actual state of cybercrime in a geographical area, or if the data collection technique is flawed, the prediction will be inaccurate. The source of the data used for the prediction is pivotal to its accuracy.

In most cases, the historical data are usually criminal justice data, which scholars have argued pose various challenges.[44] Some victims fail to report cybercrime due to embarrassment, and several cybercrime cases remain undocumented in Nigeria, making it difficult to monitor.[45] The goal of predictive policing is for law enforcement to employ proactive measures to analyse previous cybercrime data, learn trends and patterns, and spot cyber threats early enough.

It is essential to discuss the predictive policing software in order to be able to assess the potential advantages and risks of applying the model to the Nigerian cybercrime situation.

2.2 Current practice of predictive policing and its application to cybercrimes

Predictive policing for cybercrime detection involves employing AI and machine learning to ascertain patterns and trends in previous cybercrimes in an area or locality, to flag future cybercrime hotspots, and possibly to prevent them. Predictive models have been applied in different categories of cybercrime.

The linear trend and linear Holt model have been applied to cybercrime prediction and detection. Holt's linear trend method is based on exponential smoothing, which is used to predict data trends. It employs a forecast equation and two smoothing equations for the level and trend.[46] Cybersecurity experts have successfully employed AI and ML tools to understand cyber-attack threats and combat cybercrimes. For instance, "Security Orchestration Automation and Response (SOAR) tools are used by organisations to automatically correlate information from different sources and interact with security tools to remediate incidents with human intervention. AI systems are being trained to detect malicious software, run pattern recognition, and detect malware before they enter the network."[47]

---

43 Mohammed *et al* 2025 *Information Systems*.

44 Brewer *et al Cybercrime Prevention*.

45 Nwafor 2024 *International Cybersecurity Law Review* 445; Chudasama *et al* 2020 *American Journal of Computer Science and Engineering Survey* 2.

46 Yapar *et al* 2018 *Hacettepe Journal of Mathematics and Statistics* 1394-1403.

47 Deloitte 2022 https://www.deloitte.com/content/dam/assets-zone1/gh/en/docs/services/risk-advisory/2023/Nigeria-Cybersecurity-Outlook-2022.pdf.

Rahaman[48] notes the expanding threats posed by cybercriminals and stresses that the big data model helps law enforcement authorities reduce cybercrime. They propose a cybercrime detection algorithm on the Hadoop platform in big data analytics that can predict likely cybercrime. The algorithm would undergo three phases to detect cyber fraud and unethical hacking through large-scale data analysis. Massive digital records/information are collected, analysed, and visualised using big data analytics. Subsequently, it is possible to foresee and prevent cybercrime activities.[49] Several researchers have employed various algorithms to detect cybercrimes. These algorithms include unsupervised learning algorithms such as K-means, which achieve high efficiency and adequate performance, naïve Bayes, and the K-nearest neighbour (KNN).[50]

Predictive techniques such as data mining are employed to interpret and develop strategies to enhance crime prevention.[51] Data mining is the process of analysing patterns, correlations and variances within large datasets to predict outcomes and solve problems.[52] Abouzakhar *et al* developed a model to detect network cybercrimes using a Bayesian learning network. The proposed model was applied to a DARPA (Defense Advanced Research Projects Agency) 2000 dataset of DDoS (Distributed Denial of Service) attacks developed by the Massachusetts Institute of Technology (MIT) Lincoln Laboratory.[53] Benferhat, Keneza and Mokhtari proposed a naïve Bayes approach that monitors alert correlation to provide efficient algorithms for detecting and predicting future scenarios.[54] Naïve Bayes does not require extensive expert knowledge to implement. It uses historical data to build naïve Bayes models for individually observed intrusions. The authors posit that this approach is simple yet efficient for making predictions from automatically learned data-driven models rather than expert-provided ones.[55] The idea of predictive policing and law enforcement work has been described as:

> including future-orientation, scientification, rationalisation, managerialism, and, not least, a certain techno-fetishism. Moreover, it picks up and reinforces current trends towards digitalisation and datafication in policing. And at the same time, it can be considered a steppingstone towards structural reform and the large-scale integration of data and analytical tools in multipurpose platforms. Predictive policing can thus be seen as emblematic of the multiplicity of larger trajectories in police work, and insights about how

48 Rahaman 2020 *International Journal of Computer Science and Information Security*.
49 Rahaman 2020 *International Journal of Computer Science and Information Security*.
50 Al-Khater *et al* 2020 *IEEE Access*
51 Al Boom and Bin Thani *Predictive Policing*.
52 SAS date unknown https://www.sas.com/en_ca/insights/analytics/data-mining.html.
53 Al-Khater *et al* 2020 *IEEE Access* 137298.
54 Benferhat, Keneza and Mokhtari "Naïve Bayes Approach for Detecting Coordinated Attacks".
55 Benferhat, Keneza and Mokhtari "Naïve Bayes Approach for Detecting Coordinated Attacks" 704.

> predictive policing reconfigures police organisation and police practices can provide valuable indications of broader societal questions that emerge from the combination of data, algorithms, and security.[56]

Despite its shortcomings and the longstanding debate over its effectiveness and accountability, it has been argued that law enforcement bodies need to harness its positive aspects.[57]

2.2.1 Place-based prediction: The PredPol system (now rebranded Geolitica)

The PredPol model was developed by anthropologist Jeffrey Brantingham and Mathematician Andrea Bertozzi in collaboration with the Los Angeles Police Department, the FBI and the University of California, Los Angeles.[58] It is "based on equations that are used to model earthquake occurrences and chemical reactions which produce certain 'hotspots,' and where adding 'hotspot policing' can be viewed as an inhibitor to the process".[59] The PredPol model is built on the epidemic-type aftershock (ETAS) model and the reaction-diffusion model upon which it is based.[60] These models are used for time-variant earthquake forecasting and account for the spatiotemporal clustering of earthquakes based on empirical principles.[61]

The PredPol model was designed to identify geographic areas expected to experience elevated levels of criminal activity over a given period.[62] It relies on three data points to establish its predictions: crime type, crime location and crime date/time.[63] PredPol works by using "a machine-learning algorithm to calculate its predictions. Historical event datasets are used to train the algorithm for each new city (ideally, 2-5 years of data). It then updates the algorithm daily with new events as they are received from the department".[64] The data are sourced from patrol officers' crime observation reports and the records of citizens' calls for police services.[65] Burglaries, robberies and aggravated assaults are some crimes that PredPol has been used to predict.

---

56 Egbert and Leese *Criminal Future* 220.
57 Mugari and Obioha 2021 *Social Sciences* 13.
58 Saunders 2016 *American Scientist* 264-266.
59 Wong 2022 https://www-personal.umd.umich.edu/~tiananw/PredPol.pdf.
60 Johnson, McKenzie and Wong 2024 *Notices of the American Mathematical Society* 929. The mathematical underlying of the PredPol model is beyond the scope of this work.
61 Mizrahi *et al* 2024 *Bulletin of the Seismological Society of America*.
62 Bachner *Predictive Policing*.
63 Shapiro 2017 *Nature* 458-460.
64 PredPol date unknown https://www.predpol.com/how-predictive-policing-works.
65 Ballantyne 2023 https://medium.com/@neilballantyne/the-harm-that-data-do-the-case-of-predpol-17603c59a1e2.

PredPol scientists argue that the simplicity of PredPol's prediction mechanism reduces the risk of discriminatory profiling.[66] Importantly, no demographic, personally identifiable, ethnic or socio-economic information is ever used. This eliminates the possibility of civil rights or privacy violations, as occur with other intelligence-led policing models.[67] For instance, the HunchLab system has been criticised as theoretically agnostic because it starts with no hypothesis.[68]

Although the developers of PredPol claim it reduces discriminatory profiling, some commentators dispute this claim. An independent examination of PredPol crime predictions by Gizmodo found that "PredPol's algorithm relentlessly targeted the Census block groups in each jurisdiction that were the most heavily populated by people of colour and the poor, particularly those containing public and subsidised housing. The algorithm generated fewer predictions for block groups with more white residents".[69] The statistical analysis also showed that PredPol's forecasts disproportionately fell in areas where the poorest residents live.[70] This suggests that even predictive policing systems with a higher likelihood of reducing discrimination are not immune to such discrimination, given the data foundation on which they base their predictions. The solution might be to rely on actual data rather than police historical record-keeping. Additionally, an analysis of 23,631 predictions generated by Geolitica for the period of 25 February 2018 to 18 December 2018 for the Plainfield Police Department (PPD) showed that one type of crime was likely to occur in a location not patrolled by the PPD.[71] The overall success rate was less than 1%, with only one prediction aligning with reported crimes.

It is evident from the preceding that the effectiveness of the PredPol model is questionable, and transplanting it into cybercrime detection would be problematic from the outset. The software was primarily used to detect street crimes such as domestic burglaries rather than cybercrimes.

2.3 Possible advantages and risks of the cybercrime forecasting

There are potential advantages and risks associated with the hypothetical cybercrime forecasting discussed in the previous section. Despite the criticism of predictive policing in the existing literature and public media,

66 Brayne, Rosenblat and Boyd 2015 https://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf 1-11.

67 PredPol date unknown https://www.predpol.com/how-predictive-policing-works.

68 Lee, Bradford and Posh 2024 *Justice Evaluation Journal* 136.

69 Mehrotra *et al* 2021 https://gizmodo.com/how-we-determined-predictive-policing-software-dispropo-1848139456.

70 Mehrotra *et al* 2021 https://gizmodo.com/how-we-determined-predictive-policing-software-dispropo-1848139456.

71 Sankin and Mattu 2023 https://www.wired.com/story/plainfield-geolitica-crime-predictions/.

there are benefits as well as challenges, such as providing valuable resources that aid crime prevention and investigation,[72] allowing law enforcement to make better use of limited resources, enhancing situational awareness,[73] and promoting strategic planning and decision-making within law enforcement bodies.[74] However, the risks of predictive policing models are numerous and worthy of brief discussion.

2.3.1 Bias training data/lack of accuracy

There is a need to use large amounts of historical data in training machine learning algorithms. The risk of inaccurate models due to errors or the exclusion of specific information from the training data exists. It has been argued that predictive policing algorithm models lack accuracy. Richardson, Schultz and Crawford's study spotlights the reasoning behind flawed predictive algorithms, which are often clouded by what the report describes as "dirty data". It provides thus:

> These systems are built on data produced during documented periods of flawed, racially biased, and sometimes unlawful practices and policies ("dirty policing"). These policing practices and policies shape the environment and the methodology by which data is created, which raises the risk of creating inaccurate, skewed, or systematically biased data ('dirty data'). If predictive policing systems are informed by such data, they cannot escape the legacies of the unlawful or biased policing practices that they are built on. Nor do the current claims by predictive policing vendors provide sufficient assurances that their systems adequately mitigate or segregate this data.[75]

The reliability or trustworthiness of any predictive policing model depends wholly on the integrity of its usage and the quality of the data relied on for prediction. Furthermore, the data mainly focus on street crimes such as drug trafficking and theft, which are usually associated with specific demographic groups and neighbourhoods.[76] Some neighbourhoods and individuals are over-policed with excessive patrols or identity checks, exacerbating discrimination, stereotyping and criminalising certain groups or races.[77]

---

72 Schlehahn *et al* "Benefits and Pitfalls of Predictive Policing" 145-148.

73 RAND Corporation 2013 https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9700/RB9735/RAND_RB9735.pdf.

74 Ripla 2024 https://www.linkedin.com/pulse/predictive-policing-crime-prevention-andre-ripla-pgcert-91xbe?trk=public_post_feed-article-content.

75 Richardson, Schultz and Crawford 2019 *NYU L Rev* 193.

76 Rolland 2021 https://thesecuritydistillery.org/all-articles/ethics-artificial-intelligence-and-predictive-policing.

77 Asaro 2019 *IEEE Technology and Society Magazine*.

2.3.2 Accountability

Accountability is the "acknowledgement and assumption of responsibility for actions, decisions, and consequences".[78] Accountability is a prerequisite for the democratic legitimacy of law enforcement agencies. Although law enforcement requires a level of opacity to perform its duties effectively, citizens feel threatened by this secrecy and deserve to be able to hold law enforcement accountable.[79] Law enforcement institutions must close the accountability gap by explaining their exact predictive policing methods, why they were chosen, who is targeted, and for what purpose. The accountability of AI tools is closely related to transparency, a topic which is discussed below.

2.3.3 Lack of transparency

Transparency is paramount in the use of any form of intelligence-driven policing. It is documented as a requirement in most guidelines on AI. However, there is little or no information on how police departments eventually use crime predictions. For instance, transparency concerns have surrounded the New York Police Department's (NYPD) intelligence policing efforts.[80] The joint report of the United Nations Interregional Crime and Justice Research Institute and Interpol provides that AI decisions and activities must always be understandable to human users to ensure that AI respects the fundamental rights of citizens.[81] However, the complexity of AI programmes, often referred to as black boxes owing to their opacity, makes it difficult for even experts to understand them. Rolland rightly argues that "this lack of transparency leads to a lack of accountability. Without explicability, the police cannot effectively be held accountable to the public for their actions. Additionally, AI models must always be explainable and verifiable for people to trust the system and for the judiciary to be able to exercise their authority lawfully".[82]

---

78 Thomas Reuters Practical Law 2021 https://uk.practicallaw.thomasreuters.com/w-014-8164.

79 Davis *et al* 2022 *AI and Ethics* 185-198.

80 Lau 2020 https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained. The department claims it does not rely on enforcement data such as arrest data for predictive policing purposes. The Brennan Centre alleged that the NYPD was reluctant to release documentation on the agency's use of in-house algorithms and predictive policing software. The centre had to employ the force of the law before the department released some documentation on NYPD's use of algorithms.

81 UNICRI and Interpol 2019 https://unicri.org/sites/default/files/2025-06/UNICRI%20-%20Artificial%20intelligence%20and%20robotics%20for%20law%20enforcement.pdf.

82 Rolland 2021 https://thesecuritydistillery.org/all-articles/ethics-artificial-intelligence-and-predictive-policing.

The question of the extent to which transparency or explicability in the context of the AI model is achievable has been raised.[83] Larsson and Heintz posit that, although algorithmic transparency and algorithmic decision-making are standard terminologies in recent contemporary literature, they are not fully defined. There is a need for more explicit, elaborate terminology for transparency in AI to ensure its conceptualisation.[84] Felzmann *et al* highlight the intuitive desire for transparency, both prospective and retrospective, owing to the unforeseeable nature of how AI systems reach decisions.[85]

Prospective transparency is informed transparency, meaning that data controllers must inform individuals or data users of all the relevant details regarding how the data are to be processed, in clear language. Retrospective transparency can be described as retractable transparency for accountability or explainability purposes. Kossow, Windwehr and Jenkins propose technical methods to mitigate the opacity of the system. These methods include analysing input data to ensure it is not biased, flawed, or incomplete; conducting statistical analysis of the algorithmic outcome; and performing black-box/sensitivity testing.[86] It is important to note that Article 5(1)(a) of the General Data Protection Regulations[87] covers both prospective and retrospective transparency. Since the law encourages transparency in retrospect, law enforcement officers can use it to fight cybercrime. Law enforcement authorities should inform the public about their predictive policing model, their decision-making bases, and how they assess them, to ensure democratic dialogue, total transparency, and meaningful accountability and oversight in the areas they police.

2.3.4 Privacy concerns

Data collection through surveillance and intrusions into private and virtual spaces raises privacy concerns championed by civil liberties groups.[88] In the 1950s Edward Shils argued that liberal democracy focussed on safeguarding individuals' privacy and denying it to the government.[89] The opposite has occurred in recent years, as individual privacy has evaporated

---

83 Chesterman *We, the Robots?*

84 Larsson and Heintz 2020 *Internet Policy Review*.

85 Felzmann *et al* 2019 *Big Data & Society*.

86 Kossow, Windwehr and Jenkins 2021 https://knowledgehub.transparencycdn.org/kproducts/Algorithmic-Transparency_2021.pdf.

87 *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* (2016) OJ L 119 1-88.

88 Degeling and Berendt 2017 *AI and Society*.

89 Edward *Torment of Secrecy.*

and governments have grown more secretive.[90] The boom of Big Data and technology has increased the demand for political involvement in technology.[91] Robertson, Khoo and Song have provided a detailed analysis of numerous data-driven policing models used by Canadian law enforcement authorities, identifying threats to privacy, freedom of expression, arbitrary detention, etc.[92]

Data privacy has evolved to encompass a broader scope, including increased data usage and the use of cookies. Privacy policies help build consumer trust by mitigating fears that a user's data will be disclosed.[93] In the bid to mark areas with higher crime rates and make strategic predictions, law enforcement bodies breach the fundamental human rights of citizens by violating their privacy. There are also concerns regarding where the data are retained and the risk of releasing it to third parties.

2.3.5 Discrimination

Discrimination is "treating differently, without an objective and reasonable justification, persons in analogous, or relevantly similar situations".[94] AI systems can discriminate on grounds such as race, sex, gender identity, sexual orientation, ethnicity, age, religion, disability, language, nationality and social origin.[95] Mehrabi classifies discrimination as explainable and non-explainable discrimination based on the possibility of justifying or not justifying the decision/prediction produced from the triggering attributes.[96] Most data-driven algorithms rely on historical police data, extending existing racial biases in the criminal justice system to forecast crime. Critics have categorised predictive policing as a type of "tech-washing" that proclaims racially biased policing approaches to be objective since computer algorithms are perceived as replacing human judgements.[97] Varona and Suarez underscore that "discrimination has both an origin and cause of bias once the outcome of today's discriminatory decisions based on yesterday's biases populate tomorrow's datasets".[98] Most algorithms reflect the biases of the people who created them and the historical data that they rely on.

To mitigate the harm inherent in the issues raised above, the role of law enforcement officers' discretion in determining who is targeted by predictive

---

90 Chesterman *We, the Robots?*
91 Alikhademi *et al* 2022 *Artificial Intelligence and Law* 7.
92 Robertson, Khoo and Song 2020 https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf.
93 Pilton, Faily and Henriksen-Bulmer 2021 *Computers & Security* 3.
94 *Kiyutin v Russia* Application No 2700/10 ECtHR (10 March 2011) para 59.
95 Nwafor 2021 *IJLIT* 228.
96 Mehrabi *et al* 2021 *ACM Computing Surveys*.
97 Lau 2020 https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.
98 Varona and Suárez 2022 *Applied Sciences* 4.

policing and for what purpose must be addressed. The basis for a target and the reason(s) for it must be clearly explained before an individual or group is subjected to predictive policing. For instance, when a report has been made on an individual's unexplained income and lavish spending, the police can highlight such a person as a target for predictive policing. The report serves as the foundation for such a target. The purpose of predictive policing will be to determine whether the target's source of income is derived from cybercrime.

There is a low visibility of cybercrimes owing to a lack of reporting for reasons such as "the unwillingness of commercial entities, especially financial companies, to report to the police on account of reputational questions and negative publicity, due to the lack of trust in the police department".[99] Reports on cybercrime are essential for understanding patterns of cyber-attacks and improving their predictability.

Although predictive policing systems could help curb cybercrime by detecting and responding to cyberattacks promptly, in Nigeria, AI models are not employed to study previous cyberattacks or to detect future attacks.[100] The absence of a comprehensive cybercrime database would compromise the data sets used to develop predictive policing systems for Nigerian law enforcement. Additionally, the human rights and civil liberties concerns of predictive policing systems outweigh their advantages. In other words, predictive policing systems are not a reliable preventive measure for combatting cybercrime in Nigeria.

2.4 AI governance and regulatory frameworks in Nigeria

This section explores the AI regulatory framework in Nigeria to determine the legal status of AI technologies, particularly predictive policing tools, and the governance implications on risk and compliance management.

Nigeria does not have a dedicated AI legal or regulatory framework. In 2024, the Nigerian government published its draft National AI Strategy, aiming to leverage AI for socio-economic development and technological leadership. AI is governed indirectly by existing laws that cover aspects such as data protection and cybercrime. In the absence of dedicated AI regulation, this study focusses on laws relevant to predictive policing and cybercrime, including the *Nigeria Data Protection Act* and the *Cybercrime Act*, Nigeria's cyber-specific legislation.

---

99 Chudasama *et al* 2020 *American Journal of Computer Science and Engineering Survey* 2-3.

100 Nwafor *Cybercrime and the Law* 135.

3.1.1 Nigeria Data Protection Act of 2023

The *Nigeria Data Protection Act* (NDPA) of 2023 is the first law enacted to specifically govern and regulate the protection of personal data in Nigeria. It is vital legislation with legal implications for various sectors of the economy, including AI. The NDPA indirectly relates to AI, particularly concerning the automated processing of personal data. The NDPA replaced and superseded the *Nigerian Data Protection Regulation* of 2019.[101]

3.1.1.1 Relevant provisions of the NDPA on AI

(a) Automated decision-making and profiling

Section 2(1) of the NDPA provides that the Act shall apply and govern all forms of the processing of personal data, including processing by automated means. The Act restricts decisions based solely on automated processing without human intervention if such decisions produce legal or significant effects on individuals.[102] The NDPA takes a risk-based approach applicable when AI technologies are deployed to process data.

(b) Data privacy and protection principles

Section 24 of the NDPA outlines the principles of data processing and details how personal data should be processed and handled to ensure fairness, accountability, transparency and accuracy.[103] Section 24(3) provides that "Notwithstanding anything to the contrary in this Act or any other law, a data controller or data processor owes a duty of care, in respect of data processing, and shall demonstrate accountability, in respect of the principles contained in the Act."[104]

(c) Data privacy impact assessment

Section 28 of the NDPA outlines the data privacy impact assessment process required of a data controller when the processing of personal data may result in a high risk to a data subject's rights and freedoms. The primary aim of a data privacy impact assessment is to identify, assess and mitigate risks that data processing activities pose to the privacy rights and freedoms of individuals.[105] The data privacy impact assessment is a systematic description of the envisaged data processing and its purpose; an evaluation of the necessity and proportionality of the processing; an assessment of the

---

101 *Nigerian Data Protection Act*, 2023 (NDPA) s 64(2)(f).
102 NDPA s 37.
103 NDPA s 24; Nwafor 2025 *Communicatio* 96-99.
104 NDPA s 24(3).
105 Data Protection Commission date unknown https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments.

risks to the rights and freedoms of the data subject and the measures envisaged to address those risks.

(d) The Nigerian Data Protection Commission's General Application and Implementation Directive

Section 4 of the NDPA establishes the Nigerian Data Protection Commission (NDPC). The NDPC issued the Data Protection Commission's *General Application and Implementation Directive* (GAID) in 2025 to provide detailed practical guidance and a regulatory framework for implementing the NDPA. The GAID is designed to ensure uniform compliance across all sectors of the economy and to address emerging technological challenges, including AI and cross-border data transfers. The GAID primarily connects with AI through mandatory privacy-by-design requirements and specific compliance obligations for AI and other evolving technologies.

(e) Rights of data subjects

Section 34 of the NDPA grants data subjects extensive rights to ensure control, accountability, access and transparency, which impacts how AI systems operate in Nigeria. The key rights of data subjects under the NDPA include the right to be informed, the right to access, the right to rectification, the right to erasure/right to be forgotten,[106] the right to withdraw consent,[107] the right to object,[108] and data portability rights.[109] Section 37 of the NDPA outlines rights regarding automated decision-making and profiling. The Act restricts decisions based solely on automated processing without human intervention if such decisions produce legal or significant effects on individuals. The right not to be subject to purely automated decisions does not apply in the following instances:

(i) Such processing is necessary for entering or performing a contract between the data subject and a data controller.

(ii) Such processing is authorised by law, and safeguards are put in place.

(iii) The data subject has explicitly consented.[110]

This shows that no provision of the NDPA explicitly grants AI technologies, especially predictive policing, legal standing in Nigeria. However, the NDPA governs the processing of personal data, including automated processing and profiling, which are usual components of predictive policing systems. The existence and availability of data are instrumental to the development, deployment and advancement of AI systems. Data are a vital driver of an AI

106 NDPA s 34(d); Nwafor, Nwafor and Alozie 2020 *AJLS* 1-27.
107 NDPA s 35.
108 NDPA s 36.
109 NDPA s 38.
110 NDPA s 37(2).

system's quality, quantity, accuracy and results.[111] The NDPA indirectly regulates AI technologies through its robust framework, which emphasises human oversight, transparency, privacy by design, and enforcement by the NDPC. Automated processing and profiling are limited perspectives on predictive policing, a concept with a wide scope. It is important to note that the NDPA does not provide clear provisions to ensure compliance, risk management, and the technological efficiency of AI technologies, especially predictive policing systems.

3.1.2 The Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024

The *Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act* 2024 amended and expanded the *Cybercrimes (Prohibition, Prevention, etc.) Act*, 2015. The Act does not contain specific provisions regulating or bestowing legal status on AI technologies such as predictive policing. However, it targets AI-related risks through enhanced provisions that strengthen the obligation of data protection and address crimes facilitated by AI such as identity theft, fraud and hacking.

3.1.2.1 Relevant provisions of the *Cybercrime Act* with indirect implications for AI systems

(a) Protection of traffic data and subscriber information

Section 38(1) of the *Cybercrime Act*, 2024 provides that "A service provider shall keep and protect specific traffic data and subscriber information in accordance with the provision of the Nigeria Data Protection Act and as may be prescribed by the relevant authority for the time being, responsible for the regulation of communication services in Nigeria, for a period of two years."[112] The expanded protection for traffic data and subscriber information aligns with the NDPA and emphasises user privacy and security.

The *Cybercrime Act*, 2024 regulates illegal activities involving computers, networks, the internet or other technologies.[113] Technological tools used to facilitate cybercrime include AI systems, but the *Cybercrime Act* does not mention AI. In summary, AI is not directly regulated under the Act; however, the Act has some indirect implications for AI systems. The Act addresses cyber threats in general terms, including non-AI and AI-facilitated cyber-attacks. The *Cybercrime Act* appears outdated in its consideration of AI peculiarities; it does not cover AI-generated evidence or cybersecurity measures to protect AI systems. The growing threat of AI-powered

111 Nwafor 2025 *Communicatio* 93.
112 *Cybercrime Act*, 2024 s 38.
113 Nwafor 2024 *AJLS* 249-270.

cybercrime in Nigeria, including the use of automated hacking tools, deepfakes and social engineering scams necessitates a tailored AI legal and regulatory framework with explicit provisions that ensure ethical conduct, compliance, risk management and technological efficiency.

4 Conclusion

In theory a predictive policing system should make law enforcement more efficient and fairer. However, in practice this depends on several factors such as whether the predictive policing system uses data collected in a fair and unbiased manner. This study analyses predictive policing generally and considers its usefulness and challenges in detecting and preventing cybercrime. It examines the translation of existing predictive policing techniques into the Nigerian cybercrime context, while considering the human rights and civil liberties issues surrounding predictive policing systems. It conducts a criminological analysis of the law enforcement response to cybercrime in Nigeria. The study engages with the legal-technical governance dimension by exploring the legal status, compliance and risk management of AI technologies, particularly predictive policing systems in Nigerian law enforcement. The criminological analysis revealed that although there are regularities and crime patterns in cybercriminal behaviour in Nigeria that make accountable predictive policing a considerable technique for cybercrime mitigation, it is not a preventive measure for combatting cybercrime in Nigeria due to the ethical and human rights concerns embedded in such systems. AI is currently regulated indirectly and inadequately by broader existing laws, particularly the NDPA. Nigeria is in the process of developing dedicated AI regulation. The legal status of predictive policing systems in Nigeria is unclear, and compliance and risk are not systematically measured due to the lack of a binding AI governance and regulatory framework governing their legal position and use.

The study's technical and criminological findings will strengthen AI governance in Nigeria, influencing the framework's ability to meet objectives, operate ethically, and manage risks and compliance effectively.

Bibliography

Literature

Al Boom and Bin Thani *Predictive Policing*
Al Boom AA and Bin Thani SK *Predictive Policing* (MSc-thesis Rochester Institute of Technology 2022)

Alikhademi *et al* 2022 *Artificial Intelligence and Law*
Alikhademi K *et al* "A Review of Predictive Policing from the Perspective of Fairness" 2022 *Artificial Intelligence and Law* 1-17 https://doi.org/10.1007/s10506-021-09286-4

Al-Khater *et al* 2020 *IEEE Access*
Al-Khater WA *et al* "Comprehensive Review of Cybercrime Detection Techniques" 2020 *IEEE Access* 137293-137311 https://doi.org/10.1109/access.2020.3011259

Antonov *et al Predictive Policing*
Antonov L *et al Predictive Policing in the Belgian Police Service: An Explorative Research on the Interest Among Belgian Police Officers for Predictive Policing* (Bachelor's thesis VIVES University of Applied Sciences 2021)

Asaro 2019 *IEEE Technology and Society Magazine*
Asaro PM "AI Ethics in Predictive Policing: From Models of Threat to an Ethics of Care" 2019 *IEEE Technology and Society Magazine* 40-53 https://doi.org/10.1109/MTS.2019.2915154

Bachner *Predictive Policing*
Bachner J *Predictive Policing: Preventing Crime with Data and Analytics* (Washington DC Anderson 2012)

Benferhat, Keneza and Mokhtari "Naïve Bayes Approach for Detecting Coordinated Attacks"
Benferhat S, Keneza T and Mokhtari A "A Naïve Bayes Approach for Detecting Coordinated Attacks" in IEEE *COMPSAC 08: Proceedings of the 2008 32nd Annual IEEE International Computer Software and Applications Conference* (28 July-1 August 2008 Turku) 704-709 https://doi.org/10.1109/COMPSAC.2008.213

Brewer *et al Cybercrime Prevention*
Brewer R *et al Cybercrime Prevention: Theory and Applications* (Palgrave Macmillan Cham 2019)

Bruce *et al* 2024 *PLoS ONE*
Bruce M *et al* "Mapping the Global Geography of Cybercrime with the World Cybercrime Index" 2024 *PLoS ONE* 1-16 https://doi.org/10.1371/journal.pone.0297312

Chesterman *We, the Robots?*
Chesterman S *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law* (Cambridge University Press Cambridge 2021)

Chudasama *et al* 2020 *American Journal of Computer Science and Engineering Survey*

Chudasama D *et al* "Research on Cybercrime and Its Policing" 2020 *American Journal of Computer Science and Engineering Survey* 1-3

Custers "Profiling and Predictions"
Custers B "Profiling and Predictions: Challenges in Cybercrime Research Datafication" in Lavorgna A and Holt TJ (eds) *Researching Cybercrimes* (Palgrave Macmillan Cham 2021) 63-79 https://doi.org/10.1007/978-3-030-74837-1_4

Davis *et al* 2022 *AI and Ethics*
Davis J *et al* "Five Ethical Challenges Facing Data-driven Policing" 2022 *AI and Ethics* 185-198

Degeling and Berendt 2017 *AI and Society*
Degeling M and Berendt B "What is Wrong About Robocops as Consultants? A Technology-centric Critique of Predictive Policing" 2017 *AI and Society* 347-356 https://doi.org/10.1007/s00146-017-0730-7

Egbert 2018 *European Journal of Security Research*
Egbert S "About Discursive Storylines and Techno-fixes: The Political Framing of the Implementation of Predictive Policing in Germany" 2018 *European Journal of Security Research* 95-114 https://doi.org/10.1007/s41125-017-0027-3

Egbert and Leese *Criminal Future*
Egbert S and Leese M *Criminal Futures: Predictive Policing and Everyday Police Work* (Routledge London 2020) https://doi.org/10.4324/9780429328732

Felzmann *et al* 2019 *Big Data & Society*
Felzmann H *et al* "Transparency You Can Trust: Transparency Requirements for Artificial Intelligence Between Legal Norms and Contextual Concerns" 2019 *Big Data & Society* https://doi.org/10.1177/2053951719860542

Fouad, Sabbeh and Medhat 2022 *Computers, Materials & Continua*
Fouad KM, Sabbeh SF and Medhat W "Arabic Fake News Detection Using Deep Learning" 2022 *Computers, Materials & Continua* 3647-3665 https://doi.org/10.32604/cmc.2022.021449

Hobson *et al* 2023 *Journal of Experimental Criminology*
Hobson Z *et al* "Artificial Fairness? Trust in Algorithmic Police Decision-making" 2023 *Journal of Experimental Criminology* 165-189 https://doi.org/10.1007/s11292-021-09484-9

Johnson, McKenzie and Wong 2024 *Notices of the American Mathematical Society*
Johnson JD, McKenzie T and Wong TA "Predictive Policing: A Mathematical Primer" 2024 *Notices of the American Mathematical Society* 929-937

Kosiński and Krasnodebski "Crime Predicting in the Light of Police Statistics"
Kosiński J and Krasnodebski G "Crime Predicting in the Light of Police Statistics" in Jahankhani H, Jamal A and Lawson S (eds) *Cybersecurity, Privacy and Freedom Protection in the Connected World* (Springer Cham 2021) 55-65 https://doi.org/10.1007/978-3-030-68534-8_5

Larsson and Heintz 2020 *Internet Policy Review*
Larsson S and Heintz F "Transparency in Artificial Intelligence" 2020 *Internet Policy Review* 1-16 https://doi.org/10.14763/2020.2.1469

Lee, Bradford and Posh 2024 *Justice Evaluation Journal*
Lee Y, Bradford B and Posh K "The Effectiveness of Big Data-driven Predictive Policing: Systemic Review" 2024 *Justice Evaluation Journal* 127-160 https://doi.org/10.1080/24751979.2024.2371781

Mastrobuoni 2020 *Review of Economic Studies*
Mastrobuoni G "Crime is Terribly Revealing: Information Technology and Police Productivity" 2020 *Review of Economic Studies* 2727-2753

Mehrabi *et al* 2021 *ACM Computing Surveys*
Mehrabi N *et al* "A Survey on Bias and Fairness in Machine Learning" 2021 *ACM Computing Surveys* 1-35 https://doi.org/10.1145/3457607

Meijer and Wessels 2019 *International Journal of Public Administration*
Meijer A and Wessels W "Predictive Policing: Review of Benefits and Drawbacks" 2019 *International Journal of Public Administration* 1031-1039 https://doi.org/10.1080/01900692.2019.1575664

Mizrahi *et al* 2024 *Bulletin of the Seismological Society of America*
Mizrahi L *et al* "suiETAS: Developing and Testing ETAS-based Earthquake Forecasting Models for Switzerland" 2024 *Bulletin of the Seismological Society of America* 2591-2612 https://doi.org/10.1785/0120240007

Mohammed *et al* 2025 *Information Systems*
Mohammed S *et al* "The Effect of Data Quality on Machine Learning Performance on Tabular Data" 2025 *Information Systems* 1-18 https://doi.org/10.1016/j.is.2025.102549

Mugari and Obioha 2021 *Social Sciences*
Mugari I and Obioha EE "Predictive Policing and Crime Control in the United States of America and Europe: Trends in a Decade of Research and the

Future of Predictive Policing" 2021 *Social Sciences* 1-14 https://doi.org/10.3390/socsci10060234

Mulahuwaish *et al* 2025 *Computers in Human Behavior Reports*
Mulahuwaish A *et al* "A Survey of Social Cybersecurity: Techniques for Attack Detention, Evaluations, Challenges, and Future Prospects" 2025 *Computers in Human Behavior Reports* 1-33 https://doi.org/10.1016/j.chbr.2025.100668

Nwafor *Cybercrime and the Law*
Nwafor IE *Cybercrime and the Law: Issues and Developments in Nigeria* (CLDS Publishing Lagos 2022)

Nwafor 2021 *IJLIT*
Nwafor IE "AI Ethical Bias: A Case for AI Vigilantism (AILantism) in Shaping the Regulation of AI" 2021 *IJLIT* 225-240 https://doi.org/10.1093/ijlit/eaab008

Nwafor 2022 *OAU Law Journal*
Nwafor IE "Limitation of Plea Bargaining in Prosecuting Cybercrime in Nigeria" 2022 *OAU Law Journal* 1-25

Nwafor 2024 *AJLS*
Nwafor IE "Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps" 2024 *AJLS* 249-270 https://doi.org/10.1163/17087384-12340108

Nwafor 2024 *International Cybersecurity Law Review*
Nwafor IE "Cyberstalking in Nigeria: An Exploratory Study of Section 24 of the Nigerian Cybercrimes (Prohibition, Prvenetion, etc.) (Amendment) Act" 2024 *International Cybersecurity Law Review* 443-458 https://doi.org/10.1365/s43439-024-00126-0

Nwafor 2025 *Communicatio*
Nwafor IE "Cultural Diversity and Inclusivity in Africa's Internet Landscape: An Analysis of the African Union's Efforts on Data Governance" 2025 *Communicatio* 88-104 https://doi.org/10.1080/02500167.2024.2438071

Nwafor, Nwafor and Alozie 2020 *AJLS*
Nwafor IE, Nwafor N and Alozie J "Revenge Pornography in Nigeria: A Call for Legal Response and Cyber-censorship of Content by Internet Service Providers" 2020 *AJLS* 1-27 https://doi.org/10.1163/17087384-12340061

Okpe and Taya 2018 *Asian Journal of Multidisciplinary Studies*
Okpe VV and Taya SL "Political Perspective: Evaluating the Causes of Cybercrime in Nigeria" 2018 *Asian Journal of Multidisciplinary Studies* 1-12

Pericherla and Ilavarasan 2024 *International Journal of Intelligent Unmanned Systems*
Pericherla S and Ilavarasan E "Transformer Network-based Word Embeddings Approach for Autonomous Cyberbullying Detection" 2024 *International Journal of Intelligent Unmanned Systems* 154-166 https://doi.org/10.1108/ijius-02-2021-0011

Pilton, Faily and Henriksen-Bulmer 2021 *Computers & Security*
Pilton C, Faily S and Henriksen-Bulmer J "Evaluating Privacy-determining User Privacy Expectations on the Web" 2021 *Computers & Security* 1-36 https://doi.org/10.1016/j.cose.2021.102241

Rahaman 2020 *International Journal of Computer Science and Information Security*
Rahaman HA "A Proposed Model for Cybercrime Detection Algorithm Using Big Data Analytics" 2020 *International Journal of Computer Science and Information Security* 146-153

Raj *et al* 2021 *Electronics*
Raj C *et al* "Cyberbullying Detection: Hybrid Models Based on Machine Learning and Natural Language Processing Techniques" 2021 *Electronics* 1-20 https://doi.org/10.3390/electronics10222810

Richardson, Schultz and Crawford 2019 *NYU L Rev*
Richardson R, Schultz J and Crawford K "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice" 2019 *NYU L Rev* 193-233

Saunders 2016 *American Scientist*
Saunders F "First Person: Andrea L. Bertozzi and P. Jeffrey Brantingham" 2016 *American Scientist* 264-266

Schlehahn *et al* "Benefits and Pitfalls of Predictive Policing"
Schlehahn E *et al* "Benefits and Pitfalls of Predictive Policing" in IEEE *EISIC '15: Proceedings of the 2015 European Intelligence and Security Informatics Conference* (7-9 September 2015 Manchester) 145-148 https://doi.org/10.1109/EISIC.2015.29

Shapiro 2017 *Nature*
Shapiro A "Reform Predictive Policing" 2017 *Nature* 458-460

Shils *Torment of Secrecy*
Shils EA *The Torment of Secrecy: The Background and Consequences of American Security Policies* (The Free Press Glencoe 1956)

Sultan *et al* 2022 *Computers, Materials & Continua*
Sultan D *et al* "Cyberbullying-Related Hate Speech Detection Using Shallow-to-deep Learning" 2022 *Computers, Materials & Continua* 2115-2131 https://doi.org/10.32604/cmc.2023.032993

Udoh "Is the Data Fair?"
Udoh SE "Is the Data Fair? An Assessment of the Data Quality of Algorithmic Policing Systems" in Association for Computing Machinery *ICEGOV 2020: Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance* (23-25 September 2020 Athens) 1-7 https://doi.org/10.1145/3428502.3428503

Varona and Suárez 2022 *Applied Sciences*
Varona D and Suárez JL "Discrimination, Bias, Fairness, and Trustworthy AI" 2022 *Applied Sciences* 1-13 https://doi.org/10.3390/app12125826

Yapar *et al* 2018 *Hacettepe Journal of Mathematics and Statistics*
Yapar G *et al* "Modified Holt's Linear Trend Method" 2018 *Hacettepe Journal of Mathematics and Statistics* 1394-1403

Case law

Kiyutin v Russia Application No 2700/10 ECtHR (10 March 2011)

Legislation

Cybercrime Act, 2024

Cybercrimes (Prohibition, Prevention, etc.) Act, 2015

Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024

General Application and Implementation Directive, 2025

Economic and Financial Crimes Commission (Establishment) Act, 2004

Nigeria Data Protection Act, 2023

Nigerian Data Protection Regulation, 2019

International instruments

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ L 119 1-88

Internet sources

Akande 2024 https://www.pulse.ng/story/emmanuel-nwude-sold-an-imaginary-airport-for-dollar242-million-20240801043837890 77

Akande S 2024 *How Emmanuel Nwude Sold an Imaginary Airport for 242 Million Dollars* https://www.pulse.ng/story/emmanuel-nwude-sold-an-imaginary-airport-for-dollar242-million-2024080104383789077 accessed 18 April 2026

Alagic-Bowder 2022 https://www.occrp.org/en/news/nigeria-arrests-17-cybercrime-suspects
Alagic-Bowder N 2022 *Nigeria Arrests 17 Cybercrime Suspects* https://www.occrp.org/en/news/nigeria-arrests-17-cybercrime-suspects accessed 10 May 2026

Amer, Siddiqui and Athamena 2022 https://doi.org/10.21203/rs.3.rs-2184218/v1
Amer AYA, Siddiqui T and Athamena B 2022 *Detecting Cybercrime: An Evaluation of Machine Learning and Deep Learning Using Natural Language Processing Techniques on Social Network* https://doi.org/10.21203/rs.3.rs-2184218/v1 accessed 7 September 2025

Ballantyne 2023 https://medium.com/@neilballantyne/the-harm-that-data-do-the-case-of-predpol-17603c59a1e2
Ballantyne N 2023 *The Harm That Data Do: The Case of PredPol* https://medium.com/@neilballantyne/the-harm-that-data-do-the-case-of-predpol-17603c59a1e2 accessed 5 September 2025

Brayne, Rosenblat and Boyd 2015 https://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf
Brayne S, Rosenblat A and Boyd D 2015 *Predictive Policing* https://www.datacivilrights.org/pubs/2015-1027/Predictive_Policing.pdf accessed 10 May 2026

Check Point Software Technologies 2025 https://www.securitysa.com/ex/AfricanSecurityReport_2025.pdf
Check Point Software Technologies 2025 *African Perspectives on Cyber Security Report 2025* https://www.securitysa.com/ex/AfricanSecurityReport_2025.pdf accessed 10 May 2026

Daniel 2022 https://www.vanguardngr.com/2022/05/interpol-4/
Daniel S 2022 *Interpol Arrests 3 Nigerians for Online Scam* https://www.vanguardngr.com/2022/05/interpol-4/ accessed 10 May 2026

Data Protection Commission date unknown https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments
Data Protection Commission date unknown *Data Protection Impact Assessments* https://www.dataprotection.ie/en/organisations/know-your-

obligations/data-protection-impact-assessments accessed 1 September 2025

Deloitte 2022 https://www.deloitte.com/content/dam/assets-zone1/gh/en/docs/services/risk-advisory/2023/Nigeria-Cybersecurity-Outlook-2022.pdf
Deloitte 2022 *Nigeria Cybersecurity Outlook 2022* https://www.deloitte.com/content/dam/assets-zone1/gh/en/docs/services/risk-advisory/2023/Nigeria-Cybersecurity-Outlook-2022.pdf accessed 18 April 2026

Gottsegen 2023 https://builtin.com/artificial-intelligence/machine-learning-cybersecurity
Gottsegen G 2023 *Machine Learning in Cybersecurity: How It Works and Companies to Know* https://builtin.com/artificial-intelligence/machine-learning-cybersecurity accessed 2 September 2025

Interpol 2023 https://cybilportal.org/publications/african-cyberthreat-assessment-report-2023-cyberthreat-trends/
International Criminal Police Organisation 2023 *African Cyberthreat Assessment Report 2023* https://cybilportal.org/publications/african-cyberthreat-assessment-report-2023-cyberthreat-trends/ accessed 18 April 2026

Khan *et al* 2021 https://doi.org/10.21203/rs.3.rs-271920/v1
Khan IU *et al* 2021 *Securing Against DoS/DDoS Attacks in Internet of Flying Things Using Experience-based Deep Learning Algorithm* https://doi.org/10.21203/rs.3.rs-271920/v1 accessed 7 September 2025

Kossow, Windwehr and Jenkins 2021 https://knowledgehub.transparencycdn.org/kproducts/Algorithmic-Transparency_2021.pdf
Kossow N, Windwehr S and Jenkins M 2021 *Algorithmic Transparency and Accountability* https://knowledgehub.transparencycdn.org/kproducts/Algorithmic-Transparency_2021.pdf accessed 18 April 2026

Lau 2020 https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained
Lau T 2020 *Predictive Policing Explained* https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained accessed 18 April 2026Mathers 2020 https://www.independent.co.uk/news/world/middle-east/huspuppi-instagram-news-arrested-cyberscam-350-million-a9590826.html

Mathers M 2020 *Instagram Influencer "Hushpuppi" Arrested Amid Claims of E350 Million Global Cyberscam*

https://www.independent.co.uk/news/world/middle-east/huspuppi-instagram-news-arrested-cyberscam-350-million-a9590826.html accessed 10 May 2026

Mehrotra *et al* 2021 https://themarkup.org/show-your-work/2021/12/02/how-we-determined-crime-prediction-software-disproportionately-targeted-low-income-black-and-latino-neighborhoods
Mehrotra D *et al* 2021 *How We Determined Predictive Policing Software Disproportionately Targeted Low-income, Black, and Latino Neighbourhoods* https://themarkup.org/show-your-work/2021/12/02/how-we-determined-crime-prediction-software-disproportionately-targeted-low-income-black-and-latino-neighborhoods accessed 10 May 2026

PredPol date unknown https://www.predpol.com/how-predictive-policing-works
PredPol date unknown *How PredPol Work: Predictive Policing* https://www.predpol.com/how-predictive-policing-works accessed 7 September 2025

RAND Corporation 2013 https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9700/RB9735/RAND_RB9735.pdf
RAND Corporation 2013 *Predictive Policing: Forecasting Crime for Law Enforcement* https://www.rand.org/content/dam/rand/pubs/research_briefs/RB9700/RB9735/RAND_RB9735.pdf accessed 18 April 2026

Ripla 2024 https://www.linkedin.com/pulse/predictive-policing-crime-prevention-andre-ripla-pgcert-91xbe?trk=public_post_feed-article-content
Ripla A 2024 *Predictive Policing and Crime Prevention* https://www.linkedin.com/pulse/predictive-policing-crime-prevention-andre-ripla-pgcert-91xbe?trk=public_post_feed-article-content accessed 18 April 2026

Robertson, Khoo and Song 2020 https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf
Robertson K, Khoo C and Song Y 2020 *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf accessed 18 April 2026

Rolland 2021 https://thesecuritydistillery.org/all-articles/ethics-artificial-intelligence-and-predictive-policing
Rolland A 2021 *Ethics, Artificial Intelligence and Predictive Policing* https://thesecuritydistillery.org/all-articles/ethics-artificial-intelligence-and-predictive-policing accessed 10 May 2026

SailPoint 2023 https://www.sailpoint.com/identity-library/how-ai-and-machine-learning-are-improving-cybersecurity
SailPoint 2023 *Machine Learning (ML) in Cybersecurity* https://www.sailpoint.com/identity-library/how-ai-and-machine-learning-are-improving-cybersecurity accessed 18 April 2026

Sankin and Mattu 2023 https://www.wired.com/story/plainfield-geolitica-crime-predictions/
Sankin A and Mattu S 2023 *Predictive Policing Software Terrible at Predicting Crimes* https://www.wired.com/story/plainfield-geolitica-crime-predictions/ accessed 18 April 2026

SAS date unknown https://www.sas.com/en_ca/insights/analytics/data-mining.html
SAS date unknown *Data Mining: What It Is & Why It Matters* https://www.sas.com/en_ca/insights/analytics/data-mining.html accessed 10 May 2026

Simon 2025 https://www.ibm.com/new/product-blog/ai-powered-threat-intelligence-predicting-cyber-attacks-before-they-happen
Simon R 2025 *AI-powered Threat Intelligence: Predicting Cyberattacks Before They Happen* https://www.ibm.com/new/product-blog/ai-powered-threat-intelligence-predicting-cyber-attacks-before-they-happen accessed 10 May 2026

Storbeck 2022 https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf
Storbeck M 2022 *Artificial Intelligence and Predictive Policing: Risks and Challenges* https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf accessed 18 April 2026

Thomas Reuters Practical Law 2021 https://uk.practicallaw.thomasreuters.com/w-014-8164
Thomas Reuters Practical Law 2021 *Accountability Principles* https://uk.practicallaw.thomasreuters.com/w-014-8164 accessed 18 April 2026

Tidy 2024 https://www.bbc.com/news/articles/cr7rxpdyz9yo
Tidy J 2024 *Nigerian Brothers Jailed in US for Sextortion Scam Targeting Teenagers* https://www.bbc.com/news/articles/cr7rxpdyz9yo accessed 18 April 2026

Treleaven *et al* 2023 https://dx.doi.org/10.2139/ssrn.4507244
Treleaven P *et al* 2023 *The Future of Cybercrime: AI and Emerging Technologies are Creating a Cybercrime Tsunami* https://dx.doi.org/10.2139/ssrn.4507244 accessed 1 September 2025

UNICRI and Interpol 2019 https://unicri.org/sites/default/files/2025-06/UNICRI%20-%20Artificial%20intelligence%20and%20robotics%20for%20law%20enforcement.pdf
United Nations Interregional Crime and Justice Research Institute and International Criminal Police Organisation 2019 *Artificial Intelligence and Robotics for Law Enforcement* https://unicri.org/sites/default/files/2025-06/UNICRI%20-%20Artificial%20intelligence%20and%20robotics%20for%20law%20enforcement.pdf accessed 18 April 2026

Wong 2022 https://www-personal.umd.umich.edu/~tiananw/PredPol.pdf
Wong TA 2022 *The Mathematics of Policing* https://www-personal.umd.umich.edu/~tiananw/PredPol.pdf accessed 7 September 2025

List of Abbreviations

AI	artificial intelligence
AJLS	African Journal of Legal Studies
EFCC	Economic and Financial Crimes Commission
GAID	General Application and Implementation Directive
IJLIT	International Journal of Law and Information Technology
Interpol	International Criminal Police Organisation
ML	machine learning
NDPA	Nigeria Data Protection Act, 2023
NDPC	Nigerian Data Protection Commission
NYPD	New York Police Department
NYU L Rev	New York University Law Review
PPD	Plainfield Police Department
UNICRI	United Nations Interregional Crime and Justice Research Institute