International Journal of Police Science
ISSN 2771-3377 (online); ISSN 2771-3385 (print)
https://IJPS-Journal.org
Volume 4, Issue No. 2 (2025)

International Police Science Association (IPSA)

Research Article

Application of Big Data for Intelligence-led Policing among Law Enforcement Agencies in Jigawa State, Nigeria

Ukasha Ismail
Department of Sociology
Federal University Dutse, Jigawa State, Nigeria
ukashai17@gmail.com +234 70 3384 2788
ORCID:0000-0002-6128-0726

https://doi.org/10.56331/ijps.v4i2.9115

Submitted: 29 February 2024
Accepted: 28 December 2024
Published: 11 September 2025

Citation: Ismail, Ukasha. "Application of Big Data for Intelligence-led Policing among Law Enforcement Agencies in Jigawa State, Nigeria" *International Journal of Police Science* 4, no. 2 (2025). https://doi.org/10.56331/ijps.v4i2.9115

Abstract:

The emergence of big data technologies allows law enforcement agencies to gain access into voluminous information and extract relevant credible intelligence. Application of big data to generate intelligence makes policing predictive, proactive, swift and smart. This study examines the application of big data for intelligence-led policing among law enforcement agencies (LEAs) in Jigawa State, Nigeria. Using Crime Pattern Theory (CPT) as a theoretical framework, the study employs a survey research design with in-depth interviews (IDIs) as the primary data collection method. The major findings of the study reveal that LEAs do not usually apply big data technologies for intelligence gathering; databases such as National Identification Numbers (NINs), Bank Verification Numbers (BVNs), communication logs (messages and calls), records of customers' transactions with their banks and social media contents are regarded as valuable sources of intelligence; the law enforcement personnel are interested in applying big data technologies in their intelligence activities but lack the modern tools and technical know-how to do so. In view of these findings, the paper recommends that the Federal Government promote sustainable big data technologies in Nigeria by building an integrated database in the country. It also recommends that ICT-based government agencies and Non-Governmental Organizations (NGOs) should support LEAs through trainings and the provision of modern policing technologies.

Keywords: Big Data, Information, Intelligence-led Policing, Digital, Law Enforcement Agencies, Technology

Introduction

Big data is a technology driven by the proliferation of the internet, media, and the digitalization of information. It arises from the vast amount of data generated as people use digital devices and the internet for various activities, including education, transportation, communication, social interaction, election, banking, and commerce. Governments and corporations rely on big data technologies for various purposes, including economic development, healthcare, population management, social investment, security and law enforcement amongst others. In the digital era, criminals plan and perpetrate crimes online or offline with the help of digital technologies. In line with the above, Smith[1] explained that big data includes personal information, consumer transactions, and personal communications collected and stored in law enforcement databases merged with crime data, warrant information, and other police intelligence in order to introduce predictive policing and intelligence-driven strategies into policing models.

Intelligence and law enforcement activities are inseparable. Security strategies and operations such as arrests, raids, cordons and searches or rescue operations, are designed and executed using intelligence. Although, in the past, law enforcement agencies (LEAs) heavily relied on hardcopy reports and records in filling cabinets to make decisions, digital transformation introduces big data technologies that provide digital sources of intelligence. Dealing with the old-fashioned analogue databases is labor-intensive. The tendency for accuracy is also minimal due to human errors. The emergence of big data technologies, therefore, sets in a new pattern of intelligence gathering that appears a complete opposite of the past practice. According to McQuade[2] LEAs use big data to collect intelligence, share information, and analyze multiple and massive databases in order to manage diverse threats in a swift, efficient and smart manner. Big data technology allows LEAs to gain access to voluminous information that can be processed into credible criminal intelligence. Bell and Cogram[3] believed that the use of intelligence is very crucial not just as a tool for gathering evidence, but as a strategic planning resource that guides the deployment of strategies and resources. Gibbs et al.[4] argue that Intelligence-led policing is a new model in law enforcement practices. The new model is promising and thus becoming widely adopted and popularized. Jing and Guojun[5] recognized that intelligence-led policing is an important area of big data technology. It has been adopted by LEAs in the developed world. In U.S, for example, LEAs practice big data policing.[6] Conversely, Nigerian LEAs more often depend on informants and surveillance personnel as sources of intelligence. For example, The Nigeria Police Force (NPF) uses members of vigilante groups, community members and leaders; the Economic and Financial Crimes Commission (EFCC) utilizes whistleblowers; the National Drugs Law Enforcement Agency (NDLEA) also uses informants from amongst drug

traffickers and community members; the Nigeria Customs Service (NCS) plants informants on the routes that smugglers take to escape, and so on.

Presently, there are large amounts of data on social media platforms - posts, comments and the likes - that are useful to the Department of State Service (DSS) and the NPF. The Nigeria Financial Intelligence Unit (NFIU) can use bank transactions to detect fraudsters and money launderers. Electronic ticketing and passport database may be used by the Nigeria Immigration Service (NIS) to disclose the whereabouts or hideouts of suspected offenders. Communication logs (calls and messages) are stored by telecommunication companies and may be used as intelligence to trace suspects and prevent crime. The Federal Road Safety Corps (FRSC), NDLEA and NCS could generate a great deal of intelligence from biometric databases like National Identification Number (NIN), Bank Verification Number (BVN), drivers' licence and vehicle plate numbers, voter's card, commercial record and so on. It is against this background that this paper provides answers to the following research questions: (i) To what extent do LEAs in Jigawa State use big data technologies for intelligence-led policing? (ii) What are the sources of the big data in Nigeria? (iii) What are the benefits associated with the application of big data technologies for Intelligence-led policing? (iv) What challenges are militating against the application of big data technologies for intelligence-led policing?

Methods

This paper used qualitative model and descriptive survey design. A sample of twenty (20) participants was utilized for this study. Out of the sample, fifteen (15) participants were drawn from six (6) LEAs in Jigawa State, as follows: four (4) from the Nigeria Police Force (NPF), three (3) from the Nigeria Security and Civil Defence Corps (NSCDC), two (2) from the Economic and Financial Crime Commission (EFCC), two (2) from the Nigeria Immigration Service (NIS), two (2) from Nigeria Customs Service (NCS), two (2) Federal Road Safety Corps (FRSC); one (1) participant from Federal High Court, Dutse, Jigawa State, and four (4) were Information and Communication Technology (ICT) experts. The participants were selected using a purposive sampling technique.

The law enforcement personnel selected were mainly those whose routine duties are related to intelligence gathering, while few of them had worked or are currently working in administrative units. In-depth interview guide was used as instrument of data collection. The interviews were largely conducted face-to-face. Only three (3) interviews were conducted via phone calls, and two sessions were held via WhatsApp voice notes and chats. All the interviews were audio recorded with the consent of the participants. The data were collected in two weeks with the help of two research assistants. The data collected were transcribed, themed, based on the similarities, and analyzed. Some excerpts were presented verbatim.

Literature Review

Conceptualizing Big Data

Big data represents the cumulative information generated by people as they interact using digital devices.[7] Ferguson[8] pointed out that big data comes from people. They provide the building blocks of big data's power in small digital bits. This implies that big data is built as a result of human activities with digital technologies. Big data relates to application of data analytics, including data mining, data base management, artificial intelligence, and machine learning, to large digital datasets to derive meanings (Joh, 2016). In this sense, big data is not only large datasets, but meaningful one that had been sorted and analyzed. According to Brayne[9]

> [Big data] it is a data *environment* characterized by four features: it is vast, fast, disparate, and digital. First, big data analytics involve the analysis of large amounts of information, often measured in petabytes and involving tens of millions of observations. Second, big data typically involves high frequency observations and fast data processing. Third, big data is disparate - it comes from a wide range of institutional sensors and involves the merging of previously separate data sources. Fourth, big data is digital. The mass digitization of records facilitates the merging and sharing of records across institutions, makes storage and processing easier, and makes data more efficient to analyze and search remotely.

In the light of the above, big data refers to huge accumulated digital data. Big data stems from a simple idea to gather large details about the past, apply the right analytical tools to find connections and correlations, which can lead to unusually accurate predictions about the future. For instance, where and who criminals and terrorists may likely attack.[10] "By digitizing faces, communications, and patterns, law enforcement personnel will instantly and accurately be able to investigate billions of all-too- human clues".[11] In other words, big data technology is a solution to the challenges of crime investigation and prevention. However, the working definition of the term posits that big data involve the accumulation, collection and analysis of large quantity of digital data derived from diverse human activities.

Conceptualizing Intelligence-led Policing

Intelligence, in law enforcement context, denotes fore-knowledge about security threats, crimes and suspected persons. Intelligence-led policing is a new vocabulary and tactic in law enforcement practices, which is used for crime prevention and reduction.[12] As a new policing model, intelligence-led policing entails the use of criminal intelligence by LEAs to make informed strategic planning, improve efficiency and become more proactive.[13] The practice of intelligence-led policing is aimed at preventing crime before it occurs. The quality of law enforcement is now measured from an intelligence perspective. Intelligence-led policing has become the template for police operations in many countries globally.[14] . This implies that no law enforcement organization could achieve its goal without intelligence. Likewise, intelligence-led policing model encourages LEAs to collaborate with other public sector agencies and act proactively to mitigate perceived risks, and identify offenders, their locations or activities.[15] The central objective

behind intelligence-led policing is prediction of threats (crimes) and identification of offenders.

Benefits of Big Data to Intelligence-led Policing

Information Technology (IT) revolutionizes policing to become more data-driven, predictive and proactive. "Predictive policing, intelligence-driven prosecution, "heat lists" of targets, social media scraping, data mining, and a data-driven surveillance provide the first clues to how the future of law enforcement will evolve".[16] Contemporary law enforcement is a technology-driven enterprise that incorporates vast amounts of information, machine-learning algorithms, and artificial intelligence to identify and predict potential offenders. Big data technology has come into policing.[17] The techniques associated with big data produce dramatically different ways of identifying suspects.[18] It is invariably faster, accurate and cheaper compared to traditional methods. Intelligence-led policing which is driven by big data and concerned with solving problems is an important direction for future policing innovation.[19]

As criminality becomes sophisticated, so should the techniques and tools of law enforcement. Hence, big data technology characterizes policing in the twenty-first century. Ferguson[20] opined that the application of big data technologies for intelligence-led policing provides a broad definition of new law enforcement technologies with varying but increasing capabilities to collect, store, and analyze the information. LEAs now access massive amounts of data such as crime records; social service agencies such as schools, hospitals, water boards, electricity companies among others; census data; credit card records; and the dossiers assembled and sold by private data brokers.[21] Furthermore, stored DNA samples present an untapped source of big data for linking suspected persons to crime.[22] Monitoring of Social Networking Sites (SNSs), such as Facebook, LinkedIn, Instagram, and Twitter (X) can be used to populate government databases, fusion centers, or information repositories that provide and share information with government and law enforcement organizations about criminal activities or wanted persons.[23].

For "real-time surveillance and investigation", LEAs draw together a host of disparate technologies for immediate information access and large-scaling tracking like the Domain Awareness System (DAS), automated license-plate readers (ALPRs), facial recognition technology, aerial cameras and drones, and aggregated crime databases.[24] On the street, a police personnel or traffic warden uses his body-worn camera to scan a crowd. The feed is sent in real time back to the department where facial recognition and movement analysis software alerts a nearby patrol officer as to whether suspicious movements or people on watch lists have been identified.[25] These technologies and initiatives make policing activities information-based, easy and swift.

Application of big data technology avails LEAs with the opportunity to prevent crime before it occurs. It helps in identifying patterns of behaviours that are evidence of preparation to commit criminal acts, such

as suspicious transactions, travel patterns, supplies, tools, and material purchases consistent with items commonly used in some criminal behaviors.[26] LEAs are applying new data technologies to predict, prevent, and detect crime, to develop profiles of potential terrorists, and to make better informed policy choices in the domain of security and justice.[27]. With big data, police can receive real-time alerts. For example, officers can be automatically notified of events involving specific individuals, addresses, or cars.[28]. Big data analytics help police to know which crimes should be prevented, and at what point and time.[29]. Again, the power of predictive analytics can also be used to identify police misconduct or identify the underlying social and economic needs that lead to crime. This could be used to curb unethical practices such as extortion and harassment among police personnel. Similarly, Jing and Guojun[30] observed that the use of big data technology can improve the accuracy of crime prediction. Security managers test their hypotheses regarding who may likely commit crime, when and where with the help of big data technology.

Challenges Militating Against Application of Big Data for Intelligence-Led Policing

Critically viewed, the use of highly technical systems like big data analytics undermines transparency in intelligence gathering. It requires special kind of expertise, and many law enforcement personnel and administrators are not computer literate. LEAs remain largely dependent on private companies to provide technical supports, which increases chances of breach due to involvement of third party. In practice, LEAs could obtain big data technologies such as artificial intelligence (AI) and machine learning algorithms without the ability to understand and utilize them. Bambauer[31] seriously raised concern on individual's privacy and use of big data for intelligence-led policing. Accordingly, it is technically feasible, for example, to reduce auto theft drastically by putting a radio transmitter and tracking device in every car. But this might cost huge sum of money. There is also the fear that the technologies may be designed to disproportionately target minority communities by biased law enforcement personnel.[32].

Theoretical Framework

This paper is grounded in the principles of Crime Pattern Theory (CPT). This theory is relevant and applicable to the objectives of the study. Crime Pattern Theory was developed by Brantingham and Brantingham in 1984. The theory postulates that crime is the result of interaction of people (both offenders and potential victims) and their movements in space or time. The theory focused on patterning of crime at different levels of aggregation; the 'journey to crime', the processes by which potential offenders recognize potential crime sites and specific opportunities; and the creation and maintenance of areas of criminal residence.[33]. Crime Pattern Theory emerges in the past three decades, as part of efforts in the analysis of spatial distribution of crime.[34]

The theory has three key elements. *Activity nodes:* centres of high activity where individuals spend the most of their time, such as, the home, school, work, places of entertainment and shopping areas as well as

cyberspace, and so on. *Pathways*: the routes that connect the activity nodes of a person, such as, streets, pavements or sidewalks and footpaths that may be travelled by foot, public transport or automobile. *Edge:* a boundary that cannot easily be traversed and this can be both physical and perceptual.[35]. A physical edge includes rivers, forests and bridges. A perceptual edge includes areas that people are afraid of, such as, a rival gang territory or areas with a large discrepancy in socio-economic status.

The ideas of crime pattern theory significantly inform LEAs about where policing should be regularized, for calculating large crowd of people that engage in diverse routine activities. Cyberspace is considered as the place/environment. This suggests that intelligence personnel and policy makers could acquire useful information about their targets or suspects as they leave traces each time, they carry out activities online. Crime mapping and analysis, which has become increasingly central to the work of the police and other LEAs, is much easier and accurate with the use of big data. Likewise, one of the influential tools facilitating exploration of the spatial distribution of crime has been Geographical Information Systems (GIS). It is also a data-driven activity. In relation to the activity node (in virtual communities), social media is highly frequented by internet users. Thus, social media (tweets and comments) analysis is key in identifying both potential offender and victim. Police can pose on dating sites as minors to detect and apprehend pedophiles. Electronic transactions, communication and registration produce databases which can be largely used for the purpose of intelligence on the whereabouts of suspected persons. Database of plate numbers provide insights to LEAs including the Police road safety personnel on the highways (paths) against suspected vehicles.

Crime pattern theory predicts that offenders will usually commit crimes in areas or terrain already known to them through their routine activities. The fact that individuals' online presence increases by the minute, cyberspace serve as safe haven for those with dubious intentions. The theory simplifies the works of intelligence agencies as they can gather intelligence without fear of being detected, with the use of modern devices. However, the theory fails to acknowledge that intelligence personnel could be compromised. Consequently, the possibility of harnessing the benefits associated with big data in policing becomes undermined.

Results and Analysis

This section presents findings of the study based on the objectives of this paper, which include: the use of big data for intelligence-led policing among law enforcement agencies in Jigawa State, Nigeria; sources of the big data; benefits associated with the application of big data for intelligence-led policing; and challenges militating against its application.

Usage of big data technology for intelligence-led policing

When asked about the use of big data technology for intelligence-led policing, 8 personnel of law

enforcement agencies (LEAs) in Jigawa State opined that they do rarely use the technology. In line with this, a participant stated that:

> Yes, of course, in terms of intelligence gathering, we do use big data, either to extract information or in terms of our intelligence activities, and we are getting positive results **(01/IDI/[2]Nigeria Police Force/Inspector/2023).**

Another respondent shares the same view with the above as follows:

> We have limited access to digital evidence or intelligence. You know we are just starting. Thus, we majorly rely on manual sources of intelligence. That is physical surveillance and information received from our informants **(02/IDI/[1]NSCDC personnel/Superintendent of Corps/2023).**

In contrast, most of the participants revealed that they do not utilize big data for intelligence gathering. This was vindicated in the submissions of a participant below:

> Jigawa state police command is largely relying on human sources of intelligence. For example, we receive information from informants and we have personnel in plain-clothes that gather intelligence about some specific individuals or even at public places **(03/IDI/[1]Nigeria Police Force/ Inspector/2023).**

An Information and Communication Technology (ICT) expert narrated her view in the following words:

> From what am seeing, our LEAs are not always referring to big data for intelligence gathering because they lack knowledge in the field of IT and big data technology is a new and emerging technology **(04/IDI/ICT expert/Female/2023).**

In view of the above, it is apparent that LEAs in Jigawa State do not mostly engage in big data surveillance to gather intelligence. The implication of the low use of big data for intelligence is that the LEAs may find it difficult to handle the numerous cases reported to them for investigation.

Sources of the Big Data (databases)

Most of the participants demonstrated divergent views on various source of big data that are useful for intelligence-led policing. For example, a participants reported that:

> In fact, all databases are of relevance for intelligence gathering by the police. But the major sources of big data that we can use in Jigawa State police command are records of bank transactions or footage of Close Circuit Television (CCTV) (from commercial banks), including records of phone communication (from telecommunication companies, especially, MTN, Glo and Airtel). We can go for big data while handling cases of kidnapping, Online Advance Fee Fraud, cyber stalking and the like. We can obtain Court Order compelling the handlers of the databases to give us the data we need for our investigation (**05/IDI/[1]Nigeria Police Force/Inspector/2023).**

When a legal practitioner was asked about the sources of big data, he replied, thus:

> The most important data is data subject. There should be surveillance of the data subject. However, data subject has certain protections, which are constitutional. The constitution guards the personal data of individuals under right to privacy. There is limited capacity to which someone will apply for data subject of another, especially if it has nothing to do with allegation of crime (**06/IDI/Legal practitioner/Male/2023**)

However, more than half of the participants (11), including four (4) ICT experts, believed that Bank Verification Number, National Identification Number, and communication records made up a substantial amount of big data in Nigeria. One of the participants revealed that:

> I know that all those information that people submitted in digital form, especially with

> biometrics, from commercial Banks, National Identification Number Management, Independent, Driver's License, Passport details and so on, are key to investigation of crime. However, we only use social media to monitor what people post on their timelines. When people make derogatory posts on social media, we call them to this office (Intelligence Unit) for questioning. Also, peoples' communications are kept by their network providers. We use such to gain intelligence as well **(07/IDI/[1]NSCDC personnel/Superintendent of Corps/2023).**

In the same direction with the above, a police intelligence officer added that,

> You can agree with me that today there are other sources of electronic information such as BVN, NIN, SIM card details etc. Through them we usually get details of whoever come to our net. Just last month, on the issue of kidnapping, the first information police received about the targets was from social media; their contact details were generated. Secondly, we got their bank transactions. Again, the police were able to get their NIN. That was how the police got them tracked and apprehended **(08/IDI/[2]Nigeria Police Force/Inspector/2023).**

Another participant elaborates, thus:

> I know that all those information that people submitted in digital form, especially with biometrics, from commercial Banks, National Identification Number Management, Independent, Driver's License, Passport details and so on, are key to investigation of crime. However, we only use social media to monitor what people post on their timelines. When people make derogatory posts on social media, we call them to this office (Intelligence Unit) for questioning. Also, peoples' communications are kept by their network providers. We use such to gain intelligence as well **(09/IDI/[1]NSCDC personnel/Superintendent of Corps/2023).**

Unlike the above submissions, some participants gave their views as follows:

> Federal Road Safety Corps (FRSC) has two types of databases where it uses to trace traffic violators. The first one, they can use National Drivers' Licence (NDL). The second one, they can use Plate Number Registration because all the two contain the details of persons who have ever applied for Driver's Licence. Another one is Number Plate, which contains the details of vehicle owners **(10/IDI/Admin Officer/Federal Road Safety Corps/2023).**
>
> Nigeria Immigration Service (NIS) uses a database known as 'suspect list' forwarded by DSS to identify wanted persons. Whenever a citizen comes for passport, the passport officer of the command checks his or her name in the suspect list to track suspected criminals. It does not take time to crosscheck the suspect list. And if the network is bad, the passport officer sends it to the National headquarters Abuja. He could receive feedback in less than 15 minutes. Another way the service uses big data technology is verification of indigenization through BVN check **(11/IDI/NIS personnel/Assistant Superintendent of Immigration/Male/2023).**

The above submissions indicate that even though the LEAs do not mostly utilize big data technology for intelligence-led policing, Bank Verification Numbers, National Identification Numbers, Communication logs, Driver's Licence, and other biometric databases, social media and so on would be of great advantages to them. This implies that the LEAs have useful sources of electronic data but they do not utilize them.

Benefits Associated with the Application of Big Data Technology for Intelligence-led Policing

The participants drawn from various LEAs each expressed the benefits of the application of big data for intelligence-led policing in line with their responsibilities. For instance, three (3) police personnel and four (4) ICT experts interviewed acknowledged that the application of big data empowers the Jigawa State command and Nigeria Police Force in general with detailed, timely and accurate information about their targets. Particularly, a participant opined that:

> Before we start using modern technologies, it was difficult for us to get our targets. Sometimes, you will not even track them, and that is how many cases died [closed]. Nowadays, we derive a lot of benefits using big data because at times before swinging into action, you have already known the name of your target, his location, his associates, what he does, including his picture. Many people think of DCP Abba Kyari – Commander, Intelligence Response Team (IRT) is a magician for his remarkable successes in apprehending top criminals. The secret to his success is application of big data. So, the use of big data made our work [intelligence activities] very, very easy **(12/IDI/^{2}Nigeria Police Force/Inspector/Male/2023)**

In addition, eleven (11) participants remarked on how the application of big data technology helps LEAs to preempt crime before occurring. One senior officer from the Nigeria Security and Civil Defence Corps (NSCDC) narrates that:

> If you gather intelligence, you become proactive. It makes collection of evidence very easy for us. Application of big data makes all these possible **(13/IDI/^{2}NSCDC personnel/ Deputy Superintendent of Corps/2023).**

The Nigeria Immigration Service has acquired a new technology, which can be used by all LEAs in Nigeria as a source of intelligence. During interview with one Immigration officer, he revealed that:

> All security agencies in Nigeria could derive relevant data from "technology building" [a database owned by Nigeria Immigration Service]. All border activities are monitored by the new technology because information and photographs of anyone that goes out or comes into the country can be recorded. The technology was powered by Huawei Technology Company. It was expected to use satellite imagery to gain intelligence on border activities **(14/IDI//NIS personnel/Assistant Superintendent of Immigration/2023)**

Two (2) participants commented on the benefits of big data in relation to monitoring people's online activities. A legal practitioner indicated that:

> The use of big data technology for intelligence gathering would give LEAs the opportunity to monitor activities of people with online presence. Once the agencies have access to information of people online, they can be able to monitor their activities (**15/Legal Practitioner/Male/2023**).

In harmony with the above, a participant added that: LEAs could resort to social media censorship to monitor cybercrimes. **(16//ICT expert/Male/2023)**

The result of this analysis showed that all LEAs require application of big data for optimal performance. Any LEA that applies big data would become predictive, proactive and smart in its policing activities.

Challenges Militating against Application of Big Data Technology for Intelligence-led Policing

There are many challenges that hinder the efficient application of big data for purposes related to intelligence gathering and policing. During in-depth interview sessions, all the twenty (20) participants stated that lack of skills or knowledge of computer and other modern technologies as well as lack of the relevant technologies are among the major challenges affecting the use of big data technology for intelligence-led policing in Jigawa state. A participant revealed thus:

> We are facing many challenges to get access to the big data. For example, you can secure court order, still some commercial Banks will not be willing to release the data required. Or they may delay the process. Sometimes, it will take months before giving us the data. They used to give us excuses like they have not receive directive from their Headquarters

> and so on. This significantly affects our intelligence gathering and investigation activities **(17/IDI/[1]Nigeria Police Force/Inspector/2023).**

Furthermore, some participants highlighted some peculiar challenges. For instance, an ICT expert argued that:

> Lack of access to big data itself. In Nigeria, we do not have encouraging big data because we do not value data. So, most of our data are not gathered or harnessed. So, we do not even respect data, not to talk of keeping them for positive use such as intelligence gathering **(18/ICT expert/Female/2023).**

To put it differently, three (3) participants believed that criminals mislead law enforcement personnel by submitting inaccurate bio-data while filling forms online or creating social media accounts. They employ this strategy in order to avoid being traced, identified and apprehended. In this regard, an officer of NSCDC submits that:

> The major challenge is the issue of "pre-registered SIMs". Criminals use SIM cards that are not officially registered. Or they give incorrect name, address, and photographs to disguise. And, of course, it is difficult to trace offenders that used incorrect personal data. We have so many cases uncompleted because pre-registered SIMs were used **(19/IDI/[1]NSCDC Personnel/Superintendent of Corps/2023).**

Another respondent from the EFCC pointed out the possibility of compromise if the welfare of law enforcement personnel is not taken care of. He narrated as follows:

> There is challenge of poor remuneration for personnel. Imagine us dealing with cases related to huge amount of money. This year EFCC remitted over one trillion naira. If government does not improve our welfare, there may be compromised from some personnel **(20/IDI/EFCC personnel/2023).**

Similarly, an ICT expert opines that:

> Lack of comprehensive Database in Nigeria is one big challenge against application of big data for intelligence-led policing. Supposed the National Identification Management Commission (NIMC) is a complete database for Nigerians, biometrics of suspected criminals can be run in search for a match. It would ease the work of the police (**21/IDI/ICT expert/Male/2023**).

Discussion

This study examines the application of big data for intelligence-led policing among law enforcement agencies (LEAs) in Jigawa State, Nigeria. The data revealed low utilization of technology sources for intelligence gathering. It was also found that these agencies still rely heavily on informants or human sources of intelligence. This is too far from the view of Lamdan[36] that contemporary law enforcement is ought to be a technology-driven enterprise that incorporates vast amounts of information, machine-learning algorithms, and artificial intelligence to identify and predict potential offenders. This shows how LEAs in Jigawa State are lagging in harnessing the potentials of big data to generate intelligence. Notwithstanding this finding, the study also reveals that the Nigeria police force sometimes uses big data for intelligence from gathering.

Furthermore, the findings showed that transaction records commercial banks, Bank Verification Numbers (BVNs), National Identification Numbers (NINs), social media, and communication records with

telecommunication companies are mostly used by Nigeria Police Force, Nigeria Security and Civil Defence Corps, Economic and Financial Crimes Commission in Jigawa state. These databases deal with personal data that can be used to identify, trace and apprehend crime suspects. This is closely related to the findings of McQuade[37] that U.S' LEAs now access massive amounts of data such as crimes and criminal records; social service agencies (Schools, Hospitals, Water Boards, Electricity Companies, etc.); census data; credit card records; and the dossiers assembled and sold by private data brokers. Obviously, big data is changing the way law enforcement agencies gather intelligence, which is cardinal to their fundamental duties. As people engage in technology-enabled activities, they leave traces that may be of relevance to law enforcement, policing and security.

Likewise, it was discovered that big data technologies empower LEAs in the study area to gain detailed, timely and accurate information about their targets or suspects. This, therefore, makes policing predictive, preemptive and easy. As Smith[38] pointed out, big data helps in identifying patterns of behaviours that appear to be evidence of preparation to commit criminal acts, such as suspicious transactions, travel patterns, supplies, tools, and material purchases consistent with items commonly used in some criminal behaviors. Relatedly, governments are applying new data technologies to predict, prevent, and detect crime, to develop profiles of potential terrorists, and to make better informed policy choices in the domain of security and criminal justice.[39]

The study found out that LEAs in Jigawa State lack relevant skills or trainings to use digital technologies, including big data technology. It is therefore, concluded that police personnel may have access to big data technologies without the ability to understand and utilize them. As Shapiro[40] argued, the use of big data technology requires data mining technologies such as artificial intelligence (AI) and machine learning algorithms. Thus, the inability of law enforcement personnel to use big data technology may hinder intelligence gathering in digital Nigeria. The study also revealed that the application of big data technology could be misleading in Nigeria because databases consist of incorrect personal data submitted by people of questionable character. Similarly, there is a challenge of data mismanagement in Nigeria, which frustrates law enforcement from gaining access to accurate data on their targets.

Finally, findings from the study corroborate the assumptions of Crime Pattern Theory. The study emphasizes that LEAs are availed with a number of digital data sources for effective crime prevention strategies. The theory equally stresses that Nigerian databases like social media posts, Bank Verification Number (BVN), National Identification Number (NIN), passport details and other biometric databases are important sources of criminal intelligence. Considering the theory, offenders prefer to use internet and digital technologies to perpetrate crime. It is, therefore, easy for LEAs to track, trace and apprehend them. The theory provides clues for LEAs to preempt crime at the preparatory stage. For instance, it is easy to

predict violence when blasphemous comments are made on social media platforms. Monitoring of financial transactions also allows LEAs to uncover terrorist financing.

Conclusion

Today, law enforcement agencies (LEAs) are increasingly relying on digital technologies to introduce new policing models such as intelligence-led policing (ILP). The ILP model transforms policing into proactive, swift, and smart operations. As various human activities are now carried out with the aid of digital devices, sources of criminal intelligence increasingly exist in digital form. This has given rise to the emergence of big data technologies, which serve as a bedrock for guiding LEAs in mapping out effective crime prevention strategies across many parts of the world. This study found that LEAs in Jigawa State are eager to leverage digital data from NIMC, INEC, banks, telecommunication companies, and other sources; however, they are constrained by the lack of an integrated database system, as well as limited expertise and tools. Hence, there is a pressing need to address this gap.

Recommendations

1. ICT-based government agencies such as the National Information Technology Development Agency (NITDA), the Nigerian Communications Commission (NCC), and relevant Non-Governmental Organizations (NGOs) should support law enforcement agencies (LEAs) in the application of big data technologies for intelligence-led policing.
2. There is a need for synergy and a cordial working relationship between LEAs and custodians of private databases in Nigeria, including commercial banks, Internet Service Providers (ISPs), and telecommunication companies. Such collaboration would enhance the ability of LEAs to access intelligence reports from diverse sources.
3. Law enforcement personnel require continuous training and retraining on the use of big data technologies. At present, LEAs often rely on consulting companies to extract intelligence from big data, a practice that may create loopholes and undermine effective application. Equipping personnel with the necessary digital skills is therefore paramount.
4. The Federal Government of Nigeria should establish an integrated database system to support intelligence gathering. This would enable LEAs to generate intelligence more efficiently and carry out their operations more effectively

Author biography

Ukasha Ismail served in the Nigeria Police Force before joining Federal University Dutse as a lecturer. He holds a Bachelor's degree and a Master's in Criminology and Security Studies from Federal University

Dutse and is currently a PhD candidate at Nazarbayev University (Kazakhstan). His research interests include policing, cyber criminology, and public policy.

Endnotes

[1] Robert L. Smith. "The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement." *Theory in Action* 12, no. 3 (2019): 179–184.
[2] Brendan McQuade. "World Histories of Big Data Policing: The Imperial Epistemology of the Police-Wars of U.S. Hegemony." *Journal of World-Systems Research* 27, no. 1 (2021): 19–35.
[3] Peter Bell and Mark Congram. "Intelligence-Led Policing (ILP) as a Strategic Planning Resource in the Fight against Transnational Organized Crime (TOC)." *International Journal of Business and Commerce* 2, no. 12 (2013): 15–28.
[4] Carole Gibbs, Edmund F. McGarrell, and Bailey Sullivan. "Intelligence-Led Policing and Transnational Environmental Crime: A Process Evaluation." *European Journal of Criminology* 12, no. 2 (2015): 242–59.
[5] Li Jing and Guojun Li. "Big Data-Driven Predictive Policing Innovation." Paper presented at the 7th International Conference on Energy, Environment and Sustainable Development (ICEESD 2018), 2018.
[6] Brendan McQuade. "World Histories of Big Data Policing, 31.
[7] Bart van der Sloot, Dennis Broeders, and Erik Schrijvers, eds. *Exploring the Boundaries of Big Data.* Amsterdam: Amsterdam University Press, 2016..
[8] Andrew Guthrie Ferguson. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement.* New York: New York University Press, 2017.
[9] Sarah Brayne. "Big Data Surveillance: The Case of Policing." *American Sociological Review* 82, no. 5 (2017): 977–1006.
[10] Jonas Lerman. "Big Data and Its Exclusions." *Stanford Law Review Online* 66 (2013): 55–63.
[11] Andrew Guthrie Ferguson. *The Rise of Big Data Policing, 43*
[12] Jerry H. Ratcliffe. "Intelligence-Led Policing and the Problems of Turning Rhetoric into Practice." *Policing and Society* 12, no. 1 (2002): 53–66.
[13] Carole Gibbs, Edmund F. McGarrell, and Bailey Sullivan. "Intelligence-Led Policing and Transnational Environmental Crime, 21.
[14] Bart van der Sloot, Dennis Broeders, and Erik Schrijvers, eds. *Exploring the Boundaries of Big Data.* Amsterdam, 12.
[15] Mike Maguire and Tim John. "Intelligence-Led Policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK." *Policing and Society* 16, no. 1 (2006): 67–85.
[16] Andrew Guthrie Ferguson. *The Rise of Big Data Policing, 44*
[17] Jessica Lindsey and Rob Hatrick, "Book Review: Ferguson's *The Rise of Big Data Policing*," 3530.
[18] Elizabeth E. Joh. "The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing." *Harvard Law & Policy Review* 10 (2016): 15–42
[19] Li Jing and Guojun Li. "Big Data-Driven Predictive Policing Innovation."
[20] Andrew Guthrie Ferguson. *The Rise of Big Data Policing, 44*
[21] Brendan McQuade. "World Histories of Big Data Policing, 31.
[22] Elizabeth E. Joh. "Policing by Numbers: Big Data and the Fourth Amendment." *Washington Law Review* 89 (2014): 35–68.
[23] Andrew Guthrie Ferguson. *The Rise of Big Data Policing*, 171.
[24] Aaron Shapiro. "Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing." *Surveillance & Society* 17, no. 3/4 (2019): 456–72.
[25] Elizabeth E. Joh. "Policing by Numbers: Big Data and the Fourth Amendment.", 32.
[26] Robert L. Smith. "The Rise of Big Data Policing:, 171.
[27] Bart van der Sloot, Dennis Broeders, and Erik Schrijvers, eds. *Exploring the Boundaries of Big Data*.
[28] Sarah Brayne. "Big Data Surveillance: The Case of Policing." 197.

[29] Stephen E. Henderson. "A Few Criminal Justice Big Data Rules." *Ohio State Journal of Criminal Law* 15 (2017): 527
[30] Li Jing and Guojun Li. "Big Data-Driven Predictive Policing Innovation."
[31] Jane Bambauer. "The Lost Nuance of Big Data Policing." *Texas Law Review* 94 (2015): 1–50.
[32] ibid
[33] Roger Hopkins Burke. *An Introduction to Criminological Theory.* 3rd ed. Cullompton, UK: Willan Publishing, 2009..
[34] Fraser Newton and Marcus Felson. "Editorial: Crime Patterns in Time and Space: The Dynamics of Crime Opportunities in Urban Areas." *Crime Science* (2015): Article 3456.
[35] Roger Hopkins Burke. *An Introduction to Criminological Theory.*
[36] Sarah Lamdan. "When Westlaw Fuels ICE Surveillance: Legal Ethics in the Era of Big Data Policing." *New York University Review of Law & Social Change* 43 (2019): 255–93
[37] Brendan McQuade. "World Histories of Big Data Policing, 31.
[38] Robert L. Smith. "The Rise of Big Data Policing, 183.
[39] Bart van der Sloot, Dennis Broeders, and Erik Schrijvers, eds. *Exploring the Boundaries of Big Data*.
[40] Aaron Shapiro. "Predictive Policing for Reform? 469.