RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES

Social Science Journal

Use of Big Data for Preventing and Suppressing Crimes in Thailand[1]

By

Supatra Phanwichit
School of Law, Sukhothai Thammathirat Open University, Thailand
E-mail: thailawresearch@gmail.com

Abstract

Use of big data is beneficial to the judicial system in various respects, either surveillance and monitoring, prevention and suppression, detection and investigation, or evidence, especially use of big data for analysis as a tool for collecting data and analyzing risks of crimes, in order that crime prevention and suppression measures can be efficiently set in place. However, in the present, Thailand is still facing so many problems and restrictions in use of big data, for example, laws, database connection system, data collection standards, as well as readiness of the organizations and personnel. Thus, it is necessary to study innovations of the use of big data in the criminal justice systems of foreign countries and propose approaches to solving the problems and restrictions, for introducing the big data innovations and technologies to the judicial system with the respect to crime prevention and suppression, in order to minimize crimes and bring peace and safety to lives and properties of the people.

Keyword: Big Data; Crime Prevention and Suppression

Introduction

Big data is considered to be a technological innovation greatly beneficial to the current economy, because it is a tool of the public sector to efficiently drive the administration, coping up with technological changes (Chakphet, Saenpakdee, Pongsiri, Jermsittiparsert, 2020; Vasuvanich, Somjai, Rattamanee, & Jermsittiparsert, 2020). In solving problems of crimes, the use of big data as a tool to collect data and analyze risks of crimes, in order to provide with more specialized crime prevention and suppression measures. For Thailand, big data has not been practically used the criminal justice system, because it lacks definite legal mechanisms, despite the fact that big data analysis is beneficial to the judicial system in various respects, either surveillance and monitoring, prevention and suppression, detection and investigation, or evidence. As such, the public sector should pay more regards to the use of big data in the judicial system for preventing and suppressing crimes, for example, analyzing crime occurrence data, analyzing risks for anticipating crime occurrence, analyzing behaviors of the offenders and tendency of crime occurrence, detecting persons and vehicles, analyzing coordination of evidence for benefits of investigation, and at the same time, the public sector should be constantly giving regards to the people's rights to privacy, as well as creating a guarantee for the people against risks of using the data and technologies. For the said reasons, it has led to an idea of research for proposing approaches, in which the public sector can efficiently use big data for preventing and suppressing crimes, by rectifying the legal restrictions, setting directions to using data to achieve crime preventive effect, thereby focusing on the people's participation through processes of data interchange and data sharing, being aware of the guarantee for the people in relation to the right of the data owners. The scope of

[1] *This article is a publication of a research under Project on Use of Big Data for Preventing and Suppressing Crimes, whose research funds are sponsored by Thailand Science Research and Innovation (TSRI) 2021.*

the research is to analyze for setting practical directions to using big data in crime prevention and suppression, because Thailand is still lacking clarity and suffering various restrictions in the process of collecting, analyzing and managing big data. This research aims to come up with approaches to reducing legal restrictions, leading to amendments to the laws and further formulating strategies of the competent agencies, by focusing on encouraging all the people to truly participate in crime prevention and suppression, whereas the people can participate in from the processes of furnishing information, exchanging data, and using data, in a form of collaboration between the state and the individuals.

Research Methodology

The Researcher uses the methodology of collecting data as qualitative research, comprising of a documentary research, an in-depth interview, a focus group, and a seminar for hearing opinions, in order that the collected data will be qualitatively analyzed and synthesized.

1. Documentary Research

The documentary research is conducted by collecting data relevant to the research from both primary sources, comprising of statutes, ministerial regulations, rules and orders, articles of ministries, bureaus, departments or state agencies, as well as judgments, and secondary sources, comprising of textbooks on laws, research papers, textbooks, articles in journals, seminar document, and online data in a form of websites. All the relevant documents are from Thailand and foreign countries, whereas a part of the documentary research will appear in the Chapter of Literature Review, and the data will be analyzed in combination with the data from the in-depth interview and focus group.

2. In-depth Interview

The in-depth interview is conducted, whose key informants are 10 qualified authorities in total, provided that the criteria for selecting the qualified authorities as the informants were a method of purposive sampling, taking into consideration the probability of obtaining data, which comprehensively cover the significant issues relevant to the use of big data for preventing and suppressing crimes in Thailand, whereas the qualified authorities can participated in the in-depth interview either directly or through advance questionnaires, in order to obtain data for analysis in combination with data obtained from other methods.

3. Focus Group

The focus group is conducted on issues of problems with, obstacles and approaches to the use of big data for preventing and suppressing crimes in Thailand, whose areas of data collection consist of Bangkok, Chiang Mai, Chonburi, and the target groups are the stakeholders in enforcement of the laws for preventing and suppressing crimes and big data services, including digital technology agencies, criminal justice agencies, the private sector and representatives of the civil society.

4. Seminar for Hearing Opinions

The seminar for hearing opinions is conducted for presenting the study results of the research project and hearing opinions from the competent agencies and stakeholders and taking the opinions into consideration for supplementing adjustment of the final report on the research.

Results of the Research

Use of Big Data for Preventing and Suppressing Crimes in Thailand

Big data are large data sets or data in large volume, or massive data, in all subject matters, aspects, formats, which may be structured data, such as data in schedules, or semi-structured data, such as log files, or even unstructured data, such as data of correspondence through social networks, for example Facebook or Twitter, or media files, etc., and may be either intra-organizational or inter-organizational data, or any channels communicating with customers, but all of them are still primary data, which need to be processed and analyzed for generating commercial values. These data may not be in a format that a organization and instantly use, but may contain some information beneficial to the organization. (Center of Information and Communication Technology, 2020)

Presently, Royal Thai Police has introduced the information technology systems to supporting operations under its missions, comprising of: Automated Fingerprint Identification System (AFIS); Criminals Database Operating System (CDOS); Police Indentikit : Computer Assisted Suspect Sketching Outfit (PICASSO); Communications, Command, Control and Intelligence C3I System for Patrol Cars; Smart Patrol Car; Royal Thai Police Information System (POLIS); E-COP, being collection of electronic document services; I2 System, being a program for analyzing criminal networks and correlating incidences, witnesses, evidence, individuals, mobile phones, bank accounts, motor vehicles and others to be used in investigation; Closed-Circuit Television (CCTV) System; Bio-Metrics Identification System (Somyati Kampala, 2020 : 106-109) ; Criminal Record Information and Management Enterprise System (CRIMES); or the new information system of Royal Thai Police, which collect case data in details, making them highly valuable information sources. They are used in prevention, suppression, detection, investigation, comprising of system for recording ordinary criminal cases, traffic accident cases, lost property incidents, lost motor vehicle incidents, missing person incidents, dead person incidents, unidentified person incidents, modus operandi, reported incidents, system for recording and monitoring released inmates, system for issuing applications for arrest warrants, entries into wanted list and removal from wanted list, system for issuing applications such as arrest warrants, postponement of prosecution, remand, system for recording temporary release and bails, system for requesting custody and confirming custody, system for recording results of background check, and system of electronic documents (e-Form) . Office of Information and Communication Technology, 2016: 3-4)

As mentioned above, a technological system, whose forms of operations use the big data, in Royal Thai Police, is the closed-circuit television system for crime prevention. Once closed-circuit television cameras are installed in places, when individuals, who are to commit criminal offenses, notice the camera, they will be afraid of being recorded while committing the offense, and some of them do not dare to commit the offenses or give up their intent to commit the offenses. The closed-circuit television system makes big data available for analysis, and enable future prediction (Thanyawuth Akkharasomcheep, 2019: 114) , forecast of crime occurrence in each area during each period. Moreover, the closed-circuit television system helps in suppressing criminal offenders, namely, a closed-circuit television system, which records data of incidents and can trace back to the time of the offense commission and find out who was the offender, leading to swift apprehension of the suspected offender, and can be used as evidence in the proceedings, leading to conviction of the offender. (Somyati Kampala, 2020: 113-114)

Big data are beneficial to crime prevention and suppression with various respects, including detection, and the criminal record database is beneficial with this respect. With respect to investigation, the criminal record database can make reference to modus operandi of the suspect for finding out how the suspect used to commit crimes, and whether the suspect was convicted before. Apart from this, the criminal record database also helps checking indices of the criminal offenders or fugitives in the wanted list and helps checking fingerprint of corpses for investigation into subsequently finding out the offenders. And in crime prevention and suppression, the criminal record database is beneficial to making a profile of a suspect under an arrest warrant, an incarcerated inmate and a released inmate, and sending the profile to Royal Thai Police and the competent agency at the domicile of the released inmate, in order to notify the local police and record the data of the released inmate, as well as to monitor behaviors and movements of the released inmate. If the released inmate commits an offense again, the data and particulars can subsequently be used in investigation and suppression of the crime. (Phassakorn Jenpravit,2021)

Forms of and Directions to Using Big Data in Foreign Countries

Studying forms of and directions to using big data in crime prevention and suppression of the United States of America, the United Kingdom and Canada, as approaches to contemplating the relevant Thai law and for benefits in application of the big data technologies to crime prevention and suppression missions, yields the results that:

The United States of America has been using big data in the criminal justice system for so long, as in 1967, the President's Commission on Law Enforcement and Administration of Justice encouraged introduction new technologies to analysis of big data in the criminal justice system for improvement, in order to achieve more efficiency and fairness (Sarah Brayne , 2018) with various respects, for example, in surveillance and monitoring operations by the police, as well as patrol, detection and analysis of crimes, whereas the scope of operations by the police with the said respects changes according to consideration and discussion at levels of policies, laws, regulations and academic institutions, as to be suitable for circumstances in different periods. Moreover, the law enforcement officers in the criminal justice institutions in the United States of America have used technologies of artificial intelligence (AI) as tools to analyze big data for predicting crimes as a basis in operating daily routines, for example, law enforcement agencies, judges, parole boards, police commissioners, police patrolmen. Results of analysis of big data by the artificial intelligence technologies help the law enforcement officers in having information covering suspects, offenders and parolees. Particularly after the September 11 Attack or the 9/11 incident, a predictive policing theory has a major role in the intelligence operations of the United States. There have been initiatives of procedures or tactics in the law enforcement agencies, based on a predictive policing theory (Brayne, S., 2017), whereas data can be collected from sources of the public and private sectors (Sarah Brayne, 2018). Currently, the law enforcement agencies in the United States of America use big data through devices to enhance efficiency and increase reliability of the information for being used in crime prevention and suppression operations, for example, the crime information systems, software and online social media. Law enforcement officers use big data through processing by the computer systems with various respects, ranging from surveillance and monitoring operations, patrol operations, detection, crime analysis and risk management. In surveillance and monitoring operations, the operations can be separated into 2 main categories, being: directed surveillance; and dragnet surveillance (Sarah Brayne, 2018);

Canada use big data through technological innovations as tools in preventive justice operations, whereas the technological tools, which process big data in different operating systems, help supporting justice operations of law enforcement officers in carrying out their duties with 2 main respects, being: 1) provision with directive information, whose data are specified in a person based format and a place-based format, that can lead to apprehension and prosecution of the suspects, whereas the law enforcement officers can intervene changes of offenses committed by individuals, who are highly likely commit crimes in different areas (targeted intervention); and 2) provision with evidence of risks in the hearing stage Sarah (Brayne & Angèle Christin, 2020) , provided that the use of big data for interpretation or precise prediction require constant availability or collection of the big data, for example, data concerning individuals, places, as well as data collected by sensors and mobile phones, such as pattern of clicking and hitting likes on online social media (N.M. Richards and J. King, 2013 : 41-46), whereas, in processing, the artificial intelligence will compile big data into presumptive results for precise prediction and identification (E.E. Joh. , 2020 : 20-22), for example, identifying places risky of crime occurrence, categories of the predicted crimes, and individuals risky of being the victims (A.E. Waldman , 2019 : 613 – 632). The artificial intelligence system will process to make a statistical prediction, whose analysis results can identify a target and probability of crime occurrence ahead of time, enabling the police to intervene the change of crime occurrence or suppress the crime before it even happens, which is crime prevention keeping up with the situations. (W.L. Perry, B. McInnis, C.C. Price, S.C. Smith, and J.S. Hollywood., 2013)

Big data are applied to technologies for preventing and suppressing crimes, such as a predictive technology, both in law enforcement and adjudication in the criminal court (S.D. Konikoff and A. Owusu-Bemphah,2019), on the same basis as a process of prediction by human. For example, the preventive justice system in Canada, the criminal court needs to assess risks and set conditions into the crime prediction software, in order that the software can render results with respect to future behaviors of the accused (or the offender), in a temporary release, restrictions of liberty and the hearing stage (M. Purcell and M. Zaia. Prediction, 2020: 515 – 542). Apart from this, predictive technologies focus on humans as bases of data analysis for trying to identify individuals likely to involve with probable criminal activities, or to assess individuals analyzed to be to involve with probable criminal activities in the future. (K.Robertson, C. Khoo, and Y. Song., 2020) , automatically making data systematically collected and processed, such as collecting online data or physical appearance from photographs of public spaces. Some algorithmic surveillance technologies may process data already collected in the law enforcement agencies or digital working files of the police in new formats, such as use of mug-shot databases as a database for facial recognition technologies. Examples of algorithmic surveillance technologies are Automated License Plate Reader (ALPR), social media surveillance software, facial recognition technology (Clearview AI) and social network analysis.

The United Kingdom (UK) - the law enforcement agencies (LEAs) and security agencies in the United Kingdom uses big data, which are obtained from the population during the daily routine, for combating crimes and protecting the country with 3 respects, being 1) crime prevention, 2) crime detection, and 3) national security. Moreover, the advent of the digital technologies results in processing of complex big data becoming more simple and faster, in turn, giving opportunities to officers in the law enforcement agencies and national security agencies for using deep data in relation to crimes. The results, which are yielded from big data analyzed by the digital technologies, are applied to enhance efficiency in the operations.

Currently, the United Kingdom uses technologies to analyze big data, for purposes of various kinds of operations. As for crime prevention and suppression, the United Kingdom prioritizes use of technologies to analyze big data for 4 primary purposes (Alexander Babuta , 2017), being *1) predictive crime mapping*, which can identify areas likely to be crime scenes, and helps in allocation of limited resources to yield the maximum efficiency, *2) predictive analytics*, which can help identifying characteristics of individuals highly likely to commit recidivism, or qualifications that can cause offenders to be recidivists, as well as identifying characteristics of individuals highly risky of being victims of crimes, such as missing, *3) advanced analytics*, which can help the police control and use data to achieve the highest efficiency, through surveillance using technological innovations, such as records of CCTV images and videos, and automatic number plate recognition (ANPR), and *4) big data technology*, whose formats can apply to data from open source, such as, data collected from online social media, for identifying problems of crimes that may lead to subsequent development of preventive law enforcement tactics.

A major big data technology, which is used in crime prevention and suppression, is the Database system, connecting different computer systems to national databases. The computer systems include: Police National Computer (PNC), which was first built in the middle of 1970s. This database contains data of criminal records, such as convictions, cautions, final warnings, and reprimand; National DNA Database and IDENT1 Fingerprint Database, whereas these databases collect electronic data concerning DNA profiles and fingerprints collected from arrested individuals and crime scenes. In 2013, it was reported that the National DNA Database and IDENT1 Fingerprint Database contained electronic records of fingerprints and DNA materials collected from the arrested individuals in 6,737,973 profiles, and from the crime scenes in 428,634 profiles; and Police National Database (PND), whose database software was first built in 2011, for the purpose of sharing intelligence at the national level. Data, which are recorded by local police departments, are automatically updated into this database. The law enforcement officers in the United Kingdom also use the Predictive Policing Technology in various forms to collect and analyze big data for the purpose of crime prevention and suppression, for example, use of predictive policing software (The Parliamentary Office of Science and Technology ,2014) , which is an operating system processing data for forecasting crime location, whereas the law enforcement officers in the United Kingdom (UK) use this software to make patrolling decisions, and the software will predict hotspots of crimes in particular categories, including burglary; street violence; vehicle theft; anti-social behavior, whose regularity is high in the United Kingdom. The basis, on which the predictive policing software works, is to analyze the historic location data in accordance with a concept that a past crime scene is risky of hosting another crime in the future. Thus, the police patrolmen will receive data of the crime hotspots, which are analyzed by the said software, and can be used in making decisions to go on foot patrol.

Apart from these, many other technological systems are used, including: PredPol's predictive policing software (The Parliamentary Office of Science and Technology ,2014), which is a software operating on the same basis as the predictive crime mapping, namely to identify a place risky of crime occurrence by using algorithm for supporting crime prevention operations; Prospective Mapping (The Parliamentary Office of Science and Technology ,2014) software to forecast hotspots for burglary and vehicles theft; Applications (App) (Motorola Solutions , 2018) , whereas police departments in the United Kingdom are trying to adjust formats of data management for crime prevention as to be suitable for the present modern world, which is being rapidly changed by the technologies. They have developed crime prevention and suppression applications for mobile devices in several forms, such as the Pronto Crime App to record crime-related data and non-crime data, the Missing Person App, being a tool for sharing data of missing individuals to concerned parties immediately upon admitting reports on the incidents, contributing to looking up for the missing individuals in expeditious manners; the Intel App, for facilitating the front-line officers, enabling them to record and share intelligence with the competent agencies in timely fashions, as well as to issue documents in traditional fashions.

Results Summary and Discussion

Big data are beneficial as tools for preventing and suppressing crimes, with respects to detection, investigation, and evidence collection in legal proceedings, and beneficial to crime prediction, whereas the public sector can analyze big data for tendency and frequency of crimes occurring in each locality during each period, as well as analyze target victims of the crimes, enable law enforcement officers and peace officers to set directions and preventive measures against crimes as to be in line with Thailand's current strategy, which is moving toward becoming an e-Government. However, use of big data in crime prevention and suppression operations is still experiencing many problems and obstacles as follows:

1) Legal Restrictions being that, currently, Digitalization of Public Administration and Services Delivery. Act, B.E. 2562 (2019), is enacted for the state agencies to administer state affairs and render public services in convenient and efficient manners, responding to serve and facilitate the people, as well as requires the state agencies to render services and integrate public data and operations as to be coordinated and interconnected in secure manners, with good governance, whereas a key objective is to integrate databases of all state agencies in order to be a data system for benefits of the public administration, and provide with convenience for the people, and to elevate public administration and service delivery to the digital system, whose working systems and databases are interconnected between the agencies in secure, efficient, swift, open and transparent manners. Section 13 provides with the basis that,for the purpose of administering state affairs and rendering services to the people, state agencies shall ensure that there is an interconnectivity and sharing of produced and processed digital data upon a request by another state agency, with which it will be mutually integrated, whereas the state agency, which is the recipient of the digital data, shall only use the data in accordance with its objectives, for its duties, and within its powers. It shall also maintain that the data is kept securely, and that there shall be no disclosure or transfer of such data to a person without the right to access it. The said law just provides with general principles, focusing on rendering services to the people and the public data good governance. In practice, power to use and share the data is vested in the agency, who owns the data, especially collection of data in judicial agencies, where the data are used in specific manners and the subjects of the data are vulnerable groups, thus impact on rights to privacy of individuals are protected. However, the law does not definitely prescribe for use of data in crime prevention and suppression missions.

2) Application of big data analysis technologies requires massive volumes of data in varieties of subject matters, in order to predict situations of commission of offenses in different forms, of each locality and for each period, surveillance and monitoring operations, patrol, detection, risk management. Using the said massive volumes of data in varieties of subject matters, state agencies must coordinate their data with data of the private sectors and individuals. The private sector also needs to connect its data with the state agencies in some missions of public interest. Thus, it is necessary to empower an agency to access data in the private sector and share the data, and stipulate criteria for achieving practical performance.

3) Issues of impact on the rights to privacy of the owners of personal data – currently, Personal Data Protection Act, B.E. 2562 (2019), is in force to prevent breach of the rights to privacy of the personal data owners and processors in collecting, using or disclosing the personal data, and provide with regulatory mechanisms or measures in

relation to protection for personal data in general, as well as definitely provide with rights of the personal data owners under the law, whereas crime prevention and suppression operations are stipulated as cases in Sections 4 (2) and (5) to enjoy exemption of not being governed by Personal Data Protection Act, B.E. 2562. That is to say – Section 4 provides "This Act shall not apply to: ... (2) operations of public authorities having the duties to maintain state security, including financial security of the state or public safety, including the duties with respect to the prevention and suppression of money laundering, forensic science or cybersecurity; … ; [and] (5) trial and adjudication of courts and work operations of officers in legal proceedings, legal execution, and deposit of property, including work operations in accordance with the criminal justice procedure; …". However, the data controller, who enjoy the exemption, is still obliged to provide with security of the personal data, as to satisfy the standard, in order to prevent the personal data from being leaked and prevent the case of personal data breach in any forms. Presently, the standard is set by Notification of Ministry of Digital Economy and Society Regarding Standard for Maintenance of Personal Data Security, B.E. 2563 (2020), which require the data controller to provide with safeguard measures for maintaining security of personal data, covering administrative safeguard, technical safeguard physical safeguard, with respects to access control. Thus, the issues of impact on the rights to privacy of the owners of personal data are a guarantee for the people that the collected personal data will be used only in accordance with the missions, and there must always be proper safeguard measures. As such, a scope of using and sharing data among different agencies must be clearly defined, in accordance with the principle of public good governance, under Digitalization of Public Administration and Services Delivery. Act, B.E. 2562, in conjuncture with Notification of Digital Government Development Commission Regarding Public Good Governance, in order to achieve practical performance and that the state agencies shall be aware of rights of the data owners.

4) Restrictions with respects to data collection – encountered problems are problems with access to data for learning facts and offense commission, and incompleteness of the data, and problems with structures of the data. Questions are how the obtained data or leads can be extended to prove guilt of the offenders as well as report on offense commission, because Thailand's financial criminal data collection system collect the data by judicial agencies in a manner that each agency collects its own statistics through its own internal procedures, comprising of police criminal statistics, statistics of cases trialed by the court of first instance, statistics of inmates incarcerated by Department of Corrections, case statistics relating to the offenders. These statistics are collected under missions as empowered by laws of each collecting agency, and they are collected in accordance with requirements of the agency, lacking a uniform standard for data collection.

Recommendations

The Researcher propose an approach to amend Digitalization of Public Administration and Services Delivery. Act, B.E. 2562, adding a part concerning management of big data for preventing and suppressing crimes, whose essential matters are as follows:

1) Stipulate criteria for data cataloging by agencies, whose missions are to prevent and suppress crimes, including Royal Thai Police, Office of Attorney-General, Department of Special Investigation, Office of the Judiciary, Department of Corrections,

Department of Probation, Department of Juvenile Observation and Protection, for encouraging state agencies and information centers, who own the data, to catalog their significant data in a uniform standard format, in turn, enabling the data users to look up, request, access, find the sources, secrecy classification, categories, forms of data, and use all the public data. It will be a key starting point in developing use of the public data, as to achieve effectiveness, enable to integration of the services and systematic use of inter-organizational data.

2) Require the data owner agency to provide with a data service system and a central data interchange system, connecting with the public database, for regulating secrecy classification of the data, procedures for requesting the rights to access the data, mechanisms and information systems, which can be verified and can summarize statistical results with respects to requests for use of data by both internal organs and external agencies.

3) Stipulate missions of judicial agencies to systematically analyze and publicize data of criminal tendency, for the purpose of formulating policies on crimes, and enhancing efficiency in law enforcement, crime prevention and suppression, and rehabilitating offenders.

4) Authorize state agencies to access and exchange data with the private sectors, for benefits of the missions of preventing and suppressing crimes, whereas formats of access and exchange must be clearly defined, for example, conditions, terms, methods, channels of access to and exchange of the data, coordination data, etc.

5) Stipulate procedures for constantly updating the data.

As for approaches to prepare readiness of law enforcement agencies for supporting the use of big data in crime prevention and suppression, the state agencies, whose missions are to prevent and suppress crimes, must be ready for collecting big data, and must specify missions in relation to big data cataloging, as to satisfy standards stipulated by Digital Government Development Agency (Public Organization), in order that the agency, who wants to use data, know sources and formats of the data, and facilitate looking up for and using the data, in data cataloging of the agencies and the country, and encouraging disclosure and interchange of public data, and a database system and information technology system must be developed as to be sufficient for data management to efficiently connect data in the judicial system, as well as set measures, methods and procedures for maintaining security of the data in accordance with the minimum standard required by the law, for preventing illegal or unauthorized access to, breach, loss or destruction of the data, as well as develop knowledge and understanding of the operative officials in applying big data technologies to missions of the agencies.

References

A.E. Waldman. Power, process, and automated decision-making. *Fordham Law Review.* 88(2), pp. 613-632, 2019.

Alexander Babuta. (2017, September). Big Data and Policing An Assessment of Law Enforcement Requirements, Expectations and Priorities. Retrieved from Royal United Services Institute for Defence and Security Studies (RUSI),: https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf

Brayne, S. (2017, August). Big Data Surveillance : The Case of Policing, Vol. 82(5) 977–1008. Retrieved from *American Sociological Review*:

http://users.soc.umn.edu/~uggen/Brayne_ASR_17.pdf

Center of Information and Communication Technology , Office of Permanent Secretariat of Ministry of Higher Education, Science, Research and Innovation, Bid Data, browsed on the15th of December 2020, at https://www.ops.go.th/main/index.php/knowledge-base/article-pr/657-big-data.

Chakphet, T., Saenpakdee, M., Pongsiri, T., Jermsittiparsert, K. (2020). The Role of Big Data Analytics in the Relationship among the Collaboration Types, Supply Chain Management and Market Performance of Thai Manufacturing Firms. International Journal of Supply Chain Management, 9(1), 28-36.

E.E. Joh. Increasing automation in policing," *Communications of the ACM*. 63, pp. 20-22, 2020.

K. Robertson, C. Khoo, and Y. Song. "*To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*", (University of Toronto Press, Canada). 2020.

M. Purcell and M. Zaia. Prediction, prevention and proof: Artificial intelligence and peach bonds in Canada. *The Canadian Bar Review*. 98, pp. 515-542, 2020.

Motorola Solutions. (2018, July). West Yorkshire Police Transforms Front-Line Policing. Retrieved from Motorola Solutions: https://www.motorolasolutions.com/content/dam/msi/docs/en-xu/public-safety/pronto_west_yorkshire_police_case_study.pdf

N.M. Richards and J. King. *Three Paradoxes of Big Data*. Stan L Rev Online. 66, pp. 41-46, 2013.

Office of Information and Communication Technology, Royal Thai Police, *Inquiry Official Training Course Handbook*, "Use of the Criminal Data Information System of Royal Thai Police, 2016, Pages 3-4.

Phassakorn Jenpravit, Introduction to Database Building and Crime Analysis of Special Investigation Operations Center, Region 4 , https://www.dsi.go.th/th/Detail/การจัดทำฐานข้อมูลและวิเคราะห์อาชญากรรมเบื้องต้นของศูนย์ปฏิบัติการคดีพิเศษภาค-๔ , browsed on the 15th of April 2021.

S. .D. Konikoff and A. Owusu-Bemphah. (2019) . "Big Data and Criminal Justice – What Canadians Should Know" (ND) at 4, online: Broadbent Institute <www.broadbentinstitute.ca> [Konikoff & Owusu-Bemphah].".

Sarah Brayne. (2018, October). The Criminal Law and Law Enforcement Implications of Big Data. Retrieved from *Annual Review of Law and Social Science*, Vol. 14:293-308: https://www.annualreviews.org/doi/10.1146/annurev-lawsocsci-101317-030839

Somyati Kampala, Analysis, Use and Benefits on the Big Data System of Royal Thai Police, *Interdisciplinary Journal*, College of Interdisciplinary Studies, Thammasat University, Year 17, Volume 1 (January 2020 – June 2020) , Pages 106 – 109.

Thanyawuth Akkharasomcheep. (2019). *What is Big Data, What is Data Science, How to Begin with Data We Have, Who Must Be in the Team* [online. browsed on : the 20th of January 2020, at https://medium.com/@thanyavuth/bigdata-และ-data-science-คืออะไร-ทีมต้องมีใครบ้างมีข้อมูลอยู่จะเริ่มอย่างไร-2cb7fec385a3, referred in Somyati Kampala, Analysis, Use and Benefits on the Big Data System of Royal Thai Police, Page 114.

The Parliamentary Office of Science and Technology. (2014, July). Big Data, Crime and Security. Retrieved from Houses of Parliament, The Parliamentary Office of Science and Technology. POSTnote Number 470: file:///D:/P%20Pim%20big%20data/UK/Big%20Data,%20Crime%20and%20Security%20-%20UK%20Parliament%20POST-PN-470.pdf

Vasuvanich, S., Somjai, S., Rattamanee, K., & Jermsittiparsert, K. (2020). The Role of Big Data Analytics in Determine the Relationship between Green Product Innovation, Market Demand and the Performance of Motorcycle Manufacturing Firms in Thailand. International Journal of Supply Chain Management, 9(1), 37-45.

W.L. Perry, B. McInnis, C.C. Price, S.C. Smith, and J.S. Hollywood. “*Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Washington” RAND Corporation, 2013.