Pandecta Research Law Journal
ISSN 1907-8919 (Print) 2337-5418 (Online)
Vol. 20 Issue 2 (2025) 669-698
DOI: https://doi.org/10.15294/pandecta.vol19i1.20485
Available online since: June 29, 2024

The Role of Big Data in Crime Prevention and Criminal Law Enforcement: Balancing Efficiency and Personal Data Protection

Lesson Sihotang[a], July Esther✉[a], Jusnizar Sinaga[a], Yanti Tiara Br Siahaan[a], Donius Ndruru[a]

[a] Faculty of Law, Universitas HKBP Nommensen, Indonesia Universitas

✉Corresponding email: *Julyesther@uhn.ac.id*

Abstract

Crime prevention and criminal law enforcement require clear arrangements so that at the same time they can form good protection for every Indonesian citizen's personal data. The purpose of this paper is to analyse the concept of using big data in crime prevention as well as criminal law enforcement and the form of boundaries and protection of personal data in the use of big data in crime prevention as well as criminal law enforcement. To achieve the results used, the research method used is a case approach and a statutory approach. From this writing, the use of big data in the context of crime prevention and criminal law enforcement has grown rapidly along with IT advances. Big data includes the collection, analysis and processing of large and diverse amounts of information. In disclosing crime cases using big data, it must also be linked to regulations on personal data protection and the data used in case disclosure must also be guaranteed validity, so that the activities carried out do not damage the sense of justice in society

KEYWORDS *Big Data, Criminal Law, Preventation.*

I. Introduction

Personal data is closely related to the concept of personal privacy where a person has the right to close or open space in his life. This makes it even more important to maintain the confidentiality of personal data. In the context of big data, personal data management is crucial to improving the performance of companies and public bodies.[1] Personal data protection not only aims to raise awareness of the importance of maintaining personal data, but also to ensure that citizens have the right to protect themselves and increase legal awareness.

The Internet, also referred to as the connected network, serves as an electronic information and communication medium. It enables various activities and E-commerce (trade and business through electronic media), e-health, e-government, e-payment, transportation, and tourism are examples of products. In addition, the development of cloud computing, also known as cloud computing, is an application that offers considerable data storage space for part of the advancement in information and communication technology, which means collecting, storing, sharing, and analyzing data quickly among business sectors and society. It is a new era of data management known as "Big Data".

[1] Sulistianingsih, Dewi, Miftakhul Ihwan, Andry Setiawan, and Muchammad Shidqon Prabowo. "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)." *Masalah-Masalah Hukum* 52, no. 1 (2023): 98.

Information and communication technology is developing rapidly, including electronics, computers, artificial intelligence, biochemistry, construction and other fields. These technologies not only provide tools for human benefit but also enable individuals to protect their rights by analyzing and visualizing data related to these rights. The Internet of Things (IoT) is a key player in the development of big data and computer technology for various health-related tasks. From a legal and ethical perspective, the use of big data should be based on moral considerations, but recent developments have sparked debate over whether ethical considerations should be considered legal considerations. The increasing amount of data available, whether from social media, financial transactions, or IoT (Internet of Things) devices, provides deep insight into people's behavior.[2] By applying law enforcement agencies can discover advanced data analysis methods such as machine teaching and data processing potential threats and respond to them before they become bigger problems. Therefore, the utilization of Big Data in this context is not only beneficial, but also necessary.

In addition to human behavior analysis, big data frameworks leverage artificial intelligence to detect anomalies across massive datasets. Machine learning systems can identify irregular financial transactions suggestive of money laundering, unusual access

[2] Faisal, Sanapiah. *Format Penelitian Sosial*. Jakarta: RajaGrafindo Persada. (2005) : 29.

patterns indicating insider theft, or behavioral deviations potentially linked to radicalization. In the context of cybercrime, algorithms are trained to recognize phishing architectures, bot-net activities, ransomware command-and-control patterns, and the digital traces left by perpetrators on the dark web. These capabilities significantly reduce investigative time, allowing law enforcement to intervene before further harm occurs.

Advances in information and communication technology have facilitated the safeguarding of personal data and increased accessibility to it online. Indonesia has a law called the Information Technology Law (ITE Law) that is strict and legally binding in the protection of personal data online. However, this does not guarantee confidentiality. Confidentiality is an essential component of existence, especially in the contemporary digital age, where most individuals rely on continuous electronic data management. The concept and domain of confidentiality has evolved alongside technological advancements, with personal data emerging as one of the most valuable commodities.

The range of benefits in the use of Big Data analytics continues to grow as does online partner matching on matchmaking sites. Finding correlations between air quality and health conditions; or using genomic analysis to accelerate the breeding of crops such as rice for drought resistance. In marketing for example, uses of Big Data include “recommendation engines” such as those used by businesses like Netflix and Amazon to make purchases or see suggestions based on the previous interests of one customer when

compared to millions of other customer data. Interestingly, large-market retailers use algorithms to detect a woman's pregnancy by tracking purchases of items, such as unscented lotion, and use the information gathered to offer new and easily detected patron-only discounts and coupons.[3] Big Data is even able to sort through the billions of social media posts made every day.

These benefits do not end there, the utilization of big data has become a powerful force in the criminal justice system, driving investigations, solving crimes, and resulting in convictions. Big Data is not just a reactive tool - but also a proactive utility proving to be equally, if not more, valuable. While currently less used in the criminal justice system compared to consumers, Big Data has the potential for wide application with crime prevention and in incriminating or exonerating defendants. In Los Angeles, California for example police use computerized "predictive policing" to anticipate criminal activity and allocate officers and other resources accordingly. In Indonesia, of course, there are still very few sources or public knowledge about what kind of utilization of big data management by law enforcement to prevent crime and how it is managed.[4] In this research, an argument will be built about the utilization of big data in crime prevention based on existing rules and regulations, both internal and accessible to the law.

---

[3] Zarsky, Tal. "The Trouble with Algorithmic Decisions." *Science, Technology, & Law*, 14, no. 1 (2016): 45–78.

[4] Windani, Cynthia Ayu. "Strategi Dan Tantangan Predictive Policing Di Era Big Data Bagi Masyarakat Modern." *Deviance Jurnal Kriminologi* 7, no. 2 (2023): 101–20.

The integration of big data into modern law enforcement represents one of the most transformative developments in contemporary security governance. The evolution of big data analytics—from simple statistical recording to real-time predictive modeling—has allowed criminal justice systems worldwide to shift from reactive to preventive paradigms. In Indonesia, although big data utilization is still in its early phases, increasing digitalization and the rapid expansion of online activities create a compelling necessity for law enforcement agencies to adopt data-driven approaches. This shift is especially relevant in urban environments where population growth, complex mobility patterns, and rising cyber-crime present challenges that traditional policing methods can no longer adequately address.

However, despite its great benefits, the use of Big Data in a legal context also faces serious challenges. Privacy and ethical issues are among the most discussed topics. The collection of large amounts of data can risk disregarding the rights of individuals, especially if the data is used without clear consent. As a result, it is important for policymakers to formulate strict regulations to keep the use of Big Data within the legal and ethical corridors.

The era of big data is now underway, where the amount of data will increase exponentially as a result of the rapid advancement of technology. Big data is a collection of very large and complex data difficult to handle or process using conventional database

management or data processing applications.[5] It guarantees data resolution with various types of existing and new data processing programs. Bringing tangible benefits to the company.

The purpose of the research on the use of big data as an effort to prevent crime and enforce criminal law is to analyze the concept of using big data in crime prevention as well as criminal law enforcement as well as the form of boundaries and protection of personal data in the use of big data. It is hoped that this research will contribute to the development of better policies in the use of big data in Indonesia.

This type of research is known as socio-legal legal research with the nature of descriptive science that describes how current ideas relate to existing regulations in Indonesia regarding big data technology and personal data protection.

First, Problem Approach. Due to the type of legal research, three approaches are used: case approach, statutory (law) approach, and conceptual (conceptual) approach. The statutory approach takes the current laws and regulations. The case approach takes cases. This method is used to analyze, prescribe, systematize, and interpret Indonesian national legal instruments on existing concepts and regulations on the utilization of big data technology in criminal law prevention and enforcement.

[5] Enforcement Tracker. *GDPR fines and penalties database*. Diakses 19 April 2025 https://www.enforcementtracker.com/

The conceptual method is used to find theories of legal science that develop on the concepts of using big data in crime prevention and criminal law enforcement. The case approach is carried out by collecting data on criminal cases related to the use of big data in crime prevention and criminal law enforcement.

Second, source of Legal Materials. Primary legal materials, namely data related to the use of big data in the realm of criminal law in various countries or in Indonesia. Secondary legal materials include legal literature, legal articles and legislation relating to the use of big data in crime prevention and criminal law enforcement.

Third, analysis of legal materials and drawing conclusions. In this research, the ontological basis and ratio legis are sought through qualitative analysis of legal materials on the utilization of big data technology in crime prevention and criminal law enforcement, to be exhausted and presented in the form of argumentative writing to make the relationship between the two propositions clear under the law.[6] In this way, one can arrive at a conclusion.

II. The Concept of Using Big Data in Crime Prevention as well as Criminal Law Enforcement

Known as "big data", computational analysis involves more advanced methods such as machine learning, speech recognition,

national language processing, expert systems, and various tools to solve problems to tasks that require more than human intelligence. In the digital age, surveillance has become more complex and integrated. Data from various sources, such as CCTV cameras, IoT devices, and social media, can be analyzed to detect suspicious activity.[7]

Furthermore, the interaction between social media analytics and criminal investigation has become increasingly relevant. Millions of interactions occur daily across platforms such as Facebook, TikTok, Instagram, and X. These interactions offer insights into public sentiment, community tensions, gang communication patterns, and digital footprints left by offenders. Sentiment analysis tools can detect spikes in hostile language, hate speech, extremist narratives, or coordinated misinformation campaigns. Such findings provide early warnings of potential unrest or organized criminal activity. In many cases, perpetrators inadvertently expose themselves by posting incriminating photos, videos, or live-location tags, which investigators can analyze to trace networks or reconstruct timelines.

In addition, the use of video analysis and facial recognition technologies enables authorities to identify criminals more quickly and accurately, which enhances response capabilities. Big data also

[7] De Conca, Silvia. "Data Protection and Privacy: The Age of Intelligent Machines." (2018) : 404.

plays an important role in profiling criminals.[8] By collecting and analyzing demographic and behavioral data, law enforcement agencies can create profiles that aid in the investigation process. For example, data regarding the characteristics of a particular offender can be used to narrow down the search and increase the likelihood of arrest.

Predictive analytics is one of the main applications of big data in law enforcement. By analyzing historical data on crime, law enforcement agencies can predict the location and timing of future crimes. For example, algorithms can analyze previous crime trends and environmental factors to forecast crime hotspots, allowing for more efficient allocation of police resources. . Big data analytics also includes social media monitoring to understand public sentiment on security issues. By analyzing conversations on social media platforms, authorities can identify public concerns and respond with more appropriate policies. This helps in creating a better relationship between law enforcement and the community, as well as building public trust.

Another important aspect concerns spatial and temporal pattern recognition. Crime tends to cluster in specific "hotspots," and big data enables a deeper understanding of why certain areas become vulnerable. Environmental criminology teaches that crime has ecological dimensions—lighting conditions, crowd density,

[8] Dewi, Sinta. "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia." *Yustisia Jurnal Hukum* 5, no. 1 (2016): 22–30.

socio-economic indicators, accessibility to escape routes, and proximity to commercial centers all influence criminal behavior. Big data systems automatically cross-reference these ecological indicators with historical and real-time crime statistics to predict where crime is most likely to occur. This approach, known as predictive policing, allows police units to deploy personnel strategically, optimizing resource allocation and increasing the deterrent effect.

The use of big data in the context of crime prevention and criminal law enforcement has grown rapidly along with IT advances. Big data involves the collection, analysis and processing of large amounts of diverse information. Through this approach, law enforcement agencies can identify patterns of criminal behavior and take more effective measures in preventing and dealing with crime. The use of big data encourages collaboration among law enforcement agencies and other organizations. By sharing data and information, different agencies can better coordinate in handling cases involving cross-border offenses or organized crime. Integrated data-driven systems enable quick access to critical information, thereby improving responses to crime.[9]

[9] Heryana, Doni, Linda Setiawati, and Budi Suhendar. "Sistem Informasi Dan Potensi Manfaat Big Data Untuk Pendidikan." *Gunahumas Jurnal Kehumasan* 2, no. 2 (2019): 351.

One of the foundational strengths of big data in crime control lies in its ability to integrate disparate data sources into a unified analytical framework. These sources include CCTV surveillance networks, telecommunications metadata, financial transaction logs, immigration and border control systems, transportation card records, e-commerce footprints, and even satellite imaging. When processed collectively, these datasets enable sophisticated mapping of criminal tendencies, including identifying habitual zones of illicit activities, typical timelines, and behavioral cues. Authorities can thus establish crime "signatures" and link them to specific types of offenses such as burglary, kidnapping, narcotics distribution, cyber-fraud, or terrorism.

The role of big data in complex investigations such as terrorism and transnational crime is even more pronounced. Terrorist networks often communicate through encrypted applications and utilize financial technologies to obscure their transactions. Big data analytics assists authorities in uncovering hidden patterns by correlating travel data, suspicious financial activities, purchase of chemical precursors, or unusual procurement of communication tools. Even seemingly insignificant data—like recurring SIM card purchases or frequent cash withdrawals—can be crucial when pieced together through algorithmic analysis. For transnational crimes such as human trafficking, big data connects border movement patterns, hotel check-in records, CCTV images, and vehicle tracking systems across jurisdictions to dismantle international criminal syndicates.

In many cases, digital evidence is key to a successful investigation. Big data enables the collection of information from electronic devices, such as cell phones and computers, which often contain important digital footprints. Analysis of this data can reveal communications, locations and activities related to a crime, strengthening the case in court. While there are many benefits to the use of big data, challenges related to privacy and ethics cannot be ignored. Increased surveillance may pose a risk of individual privacy violations. Therefore, it is important for law enforcement agencies to implement policies that ensure ethical and transparent use of data, and protect the rights of individuals.

Nonetheless, the idea of predictive policing based on big data or computational analysis still seems to pose many problems in contemporary and democratic societies. Laws governing people's privacy rights state that the police should work harder to protect and prevent crimes without attacking the criminals themselves. This is due to the very strict policies implemented by developed countries to safeguard the privacy and use of personal data. Indonesia will soon demonstrate its capacity to protect the personal data of its citizens by passing a personal data protection policy recently. Before the Indonesian police can use this predictive policing innovation, a strong and well-established system must be built first.

Laws in Indonesia governing big data, personal data protection, and crime prevention have started to show significant development in recent years. One of the major milestones is Law

No. 27 of 2022 on Personal Data Protection (PDP Law), which is the main legal umbrella in protecting individual privacy rights. This law regulates in detail the rights of data subjects, the obligations of data controllers and processors, and administrative and criminal sanctions for violations.[10] In addition, Law No. 11/2008 on Electronic Information and Transactions (ITE) and its amendment through Law No. 19/2016, as well as Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions, also strengthen the legal framework related to data management in electronic systems. [11]However, although the normative framework is taking shape, the implementation and supervision of the use of data on a large scale (big data) still face challenges, especially related to the capacity of institutions and the low data literacy of the public.

In the context of crime prevention, big data is an important tool used by law enforcement officials for the detection and prediction of criminal offences such as terrorism, money laundering, and cybercrime. Several laws such as Law No. 5/2008 on the Eradication of the Crime of Terrorism and Law No. 8/2010 on the Prevention and Eradication of the Crime of Money Laundering (TPPU) support the utilisation of data for intelligence analysis and financial tracking. However, the utilisation of big data by the state, especially by intelligence agencies and legal authorities, has not

[10] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
[11] Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Informasi Teknologi Elektronik

been fully overseen by accountable mechanisms, thus risking violating the principles of human rights and privacy protection. The absence of an independent oversight institution that deals with data protection also weakens the position of individuals in the face of potential misuse of data by the state and the private sector.

With the PDP Law, Indonesia is starting to emulate the approach of countries such as the European Union, although the lack of an independent data protection authority is an important note, because without a strong and intervention-free supervisory institution, data protection is only normative. Therefore, in addition to accelerating the establishment of a PDP authority, Indonesia also needs to reimagine the balance between national security needs and citizens' privacy rights, ensuring that the utilisation of big data for crime prevention is transparent, proportional, and overseen by fair legal mechanisms.

Finally, public trust plays a critical role. Big data systems can only operate effectively if citizens believe that their data is used lawfully and proportionally. Excessive or unauthorized surveillance risks delegitimizing law enforcement efforts and undermining societal support. Therefore, transparency mechanisms—such as published guidelines, annual impact reports, and oversight by independent bodies—are essential to maintaining accountability.

In summary, the concept of using big data in crime prevention and criminal law enforcement reflects a multidimensional paradigm shift involving technological innovation, legal reform,

institutional modernization, and ethical governance. Big data does not merely enhance investigative efficiency but redefines the broader philosophy of policing by emphasizing prevention, precision, and digital intelligence. Indonesia stands at the threshold of this transformation, requiring robust regulatory frameworks, inter-agency cooperation, and investment in human and technological capital to ensure that big data becomes a force for justice rather than a threat to personal freedoms

III. Forms of Boundaries and Personal Data Protection in the Use of Big Data in Crime Prevention as well as Criminal Law Enforcement

In the use of big data, there are limitations including the establishment of clear and specific purposes where data must be collected and used only for the purposes of crime prevention and law enforcement. Any use of data that is not directly related to these purposes must be avoided to prevent misuse that could harm individuals. Such measures are carried out using the principle of proportionality which requires that the data collected should be relevant and not excessive compared to the purpose to be achieved. This means that law enforcement agencies must ensure that only the necessary data is collected, thereby reducing the risk of invading individuals' privacy.

In general, the data collected is data that has or is subject to copyright, database rights, moral rights, trademark rights, and

trade secret or confidential information rights. The use of personal data can lead to lawsuits filed by individuals whose data is used unlawfully. In practice, the use of data is often not with the permission of the data owner, especially with regard to personal data, the approval of data use is usually only included in the terms and conditions when someone will register (sign-up) to a particular service provider, for example, Facebook, Twitter, Yahoo (e-mail) and others. In the use of Big Data, there are legal issues that must be considered by law enforcers, namely those concerning personal data security, legal protection of data, and use by other parties, and also by social media providers themselves.

Therefore, it is essential that the consent of the individual is clear and transparent as well as providing full information on how the data will be used. Individuals should be given the opportunity to understand and consent to the use of their personal data before collection takes place. To protect the identity of individuals, data anonymization and pseudonymization processes should be implemented. Anonymization removes all information that can identify the individual, while pseudonymization disguises the identity but still allows the data to be processed. By applying these two methods, data can still be used for analysis without threatening the privacy of individuals, leaving room for law enforcement agencies to perform their duties effectively.

However, the promise of big data cannot be fully realized without institutional readiness. Indonesia faces several structural challenges in this regard. Law enforcement databases remain

fragmented, managed separately by the National Police, Attorney General's Office, Ministry of Communication and Information, Directorate General of Immigration, and other agencies. These siloed systems hinder real-time data sharing. Big data requires interoperability, standardized formats, cloud-based integration, and unified national data governance policies. Without these, data becomes underutilized or inaccessible to investigators when needed most.

At the foundational level, personal data governance is guided by the principles of legality, necessity, and proportionality. The principle of legality requires that all forms of data processing must have a firm legal basis established by legislation. In the Indonesian context, this basis is primarily found in the PDP Law, which outlines permissible grounds for data collection such as consent, contractual necessity, public interest, and law enforcement operations. However, law enforcement agencies must ensure that reliance on "public interest" does not become overly broad or vaguely interpreted. Detailed statutory guidelines should therefore clarify the limits of data access for criminal investigations.

Retention limits represent one of the most important safeguards. Personal data should be deleted once it is no longer needed for the purpose for which it was collected. Indefinite retention creates significant risks, as old datasets may be hacked, leaked, or repurposed without consent. Retention periods must be tailored to case types, with strict controls, periodic audits, and mandatory deletion protocols. Indonesia's PDP Law addresses

retention in general terms, but more specific implementing regulations are needed for law enforcement data.

Apart from being used for business and trade, Big Data can also be used appropriately to reveal crimes that occur, both conventional crimes and crimes committed in cyberspace, also known as cybercrime. The disclosure of crimes using Big Data is closely related to the development of computing and data storage technology, therefore in its implementation, it is necessary to have legal instruments that can be flexible so that they are not vulnerable to technological developments that take place continuously and cause changes in the modes and procedures of criminal acts. One of the important benefits of Big Data and Computing Technology in criminal justice is that it is now easier to store and access records. Thanks to things like social media, people are storing more than they used to. It is likely that physical copies of old photographs no longer exist or have been destroyed, but many people have posted them on Facebook. An offender may post an incident, photo or event on social media that can be traced to reveal the crime he committed and to convict or possibly exonerate him.

Moreover, big data initiatives must be accompanied by strong analytical capacity. Skilled data scientists, forensic analysts, and cybersecurity experts remain limited in number within Indonesian law enforcement institutions. Training and recruitment must be intensified to ensure that sophisticated technologies are operated by competent personnel. Equally important is the establishment of

ethics-based training modules that address algorithmic bias, privacy safeguards, and responsible surveillance.

Indonesia's approach to big data law enforcement and personal data protection has undergone significant development with the passing of Law No. 27 of 2022 on Personal Data Protection (PDP Law). This law regulates the rights of data subjects, the obligations of data controllers, and criminal and administrative sanctions for violations. Although the substance adopts many international principles such as in the GDPR, its implementation still faces challenges, especially due to the lack of an independent data protection authority, as well as limitations in law enforcement and digital literacy. In addition, there are still overlaps with other regulations such as Law No. 11/2008 on Electronic Information and Transactions (ITE) and Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions, which makes the data protection ecosystem not fully integrated and effective.[12]

The principle of necessity dictates that data collection must be essential to achieving a legitimate objective. For example, when investigating cyber fraud, accessing communication logs or bank records may indeed be necessary. However, collecting unrelated personal photos, contact lists, or social media archives without clear relevance would violate this principle. Similarly,

[12] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

proportionality requires that the extent of data collected must be balanced against the severity of the offense being investigated. Investigating minor offenses cannot justify the same level of digital intrusion as investigating terrorism or organized crime.

Security safeguards ensure that collected data is stored and processed safely. Encryption, access controls, multi-layer authentication, intrusion detection systems, and controlled data environments (such as secure forensic labs) are essential. Moreover, access logs should be reviewed regularly to ensure no unauthorized personnel retrieve or manipulate sensitive data. Data protection officers in law enforcement agencies must oversee compliance with internal data governance standards

On the other hand, the European Union through the General Data Protection Regulation (GDPR) has set high standards in personal data protection. GDPR gives individuals full control over their data and imposes strict obligations on data controllers and processors. Enforcement is also very strong with independent data protection authorities in each member state authorised to impose severe sanctions, including fines of up to billions of euros. The EU balances surveillance and privacy with the principles of 'privacy by design' and 'proportionality,' ensuring that the use of data for state security or law enforcement remains within legal limits and is closely monitored.

Consent remains a cornerstone of data protection, though its application in law enforcement scenarios differs from commercial settings. While private companies must obtain explicit consent

before processing data, law enforcement relies on statutory authority. Nevertheless, transparency regarding data usage remains important. Public guidelines should indicate what types of data law enforcement may access under different circumstances, how long data is retained, and which safeguards are in place to prevent misuse.

The establishment of clear boundaries in the use of big data for law enforcement is essential to ensuring that security measures do not compromise fundamental human rights. Personal data protection lies at the heart of democratic legal systems, and its principles must guide every stage of big data processing—from collection and storage to analysis and dissemination. Boundaries act as a safeguard against abuses of power, arbitrary surveillance, and disproportionate intrusion into private life.

Technical measures like anonymization and pseudonymization reduce privacy risks while still allowing useful analysis. For example, anonymized crime data can be used to study nationwide trends without revealing the identity of offenders or victims. Pseudonymization allows large-scale data analytics where identity is masked but can be re-identified under strict legal procedures. These tools are fundamental to preventing misuse while supporting research, policymaking, and crime prevention activities.

Unlike the European Union, the United States has a sectoral and more relaxed approach. There is no single federal law like GDPR, but various sectoral regulations such as HIPAA for healthcare and

CCPA in California for consumer protection. The US is known for giving great room for innovation and industry interests, but lacks comprehensive privacy protections. [13]Surveillance by agencies such as the NSA is also extensive, as revealed in the Edward Snowden case, showing that in many cases, state surveillance dominates over the protection of individual privacy. Transparency and accountability are key issues in the US privacy law system. Meanwhile, China has a different approach by prioritising state control. The Personal Information Protection Law (PIPL) provides restrictions to the private sector in data management, but the state retains great control over citizens' data.[14] China actively uses big data for social surveillance, including facial recognition and social credit systems. While there are regulations that appear similar to the GDPR, in practice privacy is often trumped by national security and stability interests. The state has broad access and is not always constrained by independent oversight bodies.

From the approaches taken by several countries regarding privacy monitoring and protection, there are many important lessons for Indonesia, such as the importance of building an independent and strong supervisory institution, as implemented by the European Union. In addition, transparency in data processing by the state, accountability of law enforcement officials,

[13] Nugraha, Ridha Aditya. "Perlindungan Data Pribadi Dan Privasi Penumpang Maskapai Penerbangan Pada Era Big Data." *Mimbar Hukum - Fakultas Hukum Universitas Gadjah Mada* 30, no. 2 (2018): 263.

[14] Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rusbridger, A. *NSA files decoded: What the revelations mean for you*. The Guardian. (2013) : 50.

and public involvement in data policy oversight are important elements to maintain a balance between oversight and privacy protection. Indonesia also needs to clarify the limits of data use in the context of law enforcement so as not to violate human rights. By combining strong data protection as in the EU, sector flexibility as in the US, and technology regulation as in China (without replicating its repressive approach), Indonesia can create a responsible and equitable big data system.

Finally, overall in the use of Big Data for the disclosure of criminal offences, the protection of personal data owners should not be ignored. Therefore, in drafting regulations related to the disclosure of criminal offences using Big Data, it must also be linked to regulations on the protection of personal data. In addition, the validity of the data to be used in case disclosure must also be guaranteed, so that the activities carried out do not damage the sense of social justice in society. As the basic philosophy of sociological justice, which explains that a normative entity is committed to producing a just, prosperous and happy life for humans.

IV. Conclusion

The theory of predictive policing relies on computational statistical analysis available in the concept of big data to prevent crime has been used in predictive policing to reduce random shooting cases, identify hot spots, forecast riots, predict perpetrators, and link robbery cases to areas with the highest criminal code violations. In

addition, authorities can identify criminals more quickly and accurately using video analysis and facial recognition technologies, which improves response capabilities to crimes that occur. Therefore, they need to work with IT professionals to build infrastructure and applications and use pseudonyms on the data collected for predictive analysis because the current database resides in government institutions and citizen reports still use identity cards as the primary identity, a practice that may violate people's privacy.[15] If this small problem can be solved, Indonesia should have predictive policing to maintain privacy and personal data protection.

Data accuracy is another crucial boundary. Inaccurate or outdated data can lead to wrongful arrests, flawed profiling, or biased conclusions. Big data systems must therefore incorporate rigorous data cleansing, validation, and update mechanisms. When predictive policing relies on skewed or incomplete datasets, it risks reinforcing historical injustices or misidentifying vulnerable communities as crime-prone. Indonesia must incorporate algorithmic fairness principles to ensure that automated systems do not perpetuate discrimination.

With big data analysis, law enforcement does not need to spend a lot of time finding and verifying deleted posts because deleted posts do not really disappear on the internet. In the context of online gambling law enforcement, the Subnit VC Investigator of the

[15] Kitchin, Rob. *The data revolution: Big data, open data, data infrastructures and their consequences*. Sage, 2014. 3.

Medan Police Criminal Investigation Unit can use data from the perpetrator's social media to track and collect sufficient evidence, including electronic evidence related to online gambling.[16] In disclosing crime cases using Big Data, it must also be related to regulations on personal data protection. The amount of data used in case disclosure must also be guaranteed validity, so that the activities carried out do not damage the sense of justice in society.

The Indonesian government should immediately establish a fully authorised independent oversight body to oversee the use of big data by law enforcement agencies to ensure compliance with the Personal Data Protection Law (PDP Law), while upholding the principles of accountability and transparency. In addition, the government should establish clear and standardised operational guidelines for law enforcement agencies regarding the limits, purposes and procedures of processing personal data, particularly for investigative and crime prevention purposes. It is also important to develop mechanisms for periodic audits and public reporting so that the public can access information on how their data is used by the state, as well as open effective complaint channels for victims of data abuse. To maintain public trust, the government should also involve civil society and independent experts in the policy formulation process and build a massive data literacy campaign. Other concrete recommendations include

[16] Tobing, Michael Yusuf Lumbang, Miquel Joan Markus Aruan, and Kartina Pakpahan. "Penggunaan Big Data Dalam Mengungkap Kasus Kejahatan Judi Online Di Polrestabes Medan." *Journal of Economic and Business Law Review* 3, no. 1 (2023): 1–25.

adopting anonymisation technology or strong encryption, as well as requiring law enforcement agencies to conduct a data protection impact assessment (DPIA) before accessing or processing large-scale big data. These measures will not only prevent abuse of power, but also strengthen legal legitimacy and maintain a balance between national security interests and citizens' privacy rights.

References

De Conca, Silvia. "Data Protection and Privacy: The Age of Intelligent Machines." 2018. 404.

Dewi, Sinta. "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia." *Yustisia Jurnal Hukum* 5, no. 1 (2016): 22–30. https://doi.org/10.20961/yustisia.v5i1.8712.

Enforcement Tracker. *GDPR fines and penalties database*. Diakses 19 April 2025 https://www.enforcementtracker.com/

Faisal, Sanapiah. *Format Penelitian Sosial*. Jakarta: RajaGrafindo Persada, 2005.

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rusbridger, A. *NSA files decoded: What the revelations mean for you*. The Guardian, 2013

Heryana, Doni, Linda Setiawati, and Budi Suhendar. "Sistem Informasi Dan Potensi Manfaat Big Data Untuk Pendidikan." *Gunahumas Jurnal Kehumasan* 2, no. 2 (2019): 351. https://doi.org/10.17509/ghm.v2i2.23023.

Kitchin, Rob. *The data revolution: Big data, open data, data infrastructures and their consequences*. Sage, 2014. 3.

Nugraha, Ridha Aditya. "Perlindungan Data Pribadi Dan Privasi Penumpang Maskapai Penerbangan Pada Era Big Data." *Mimbar Hukum - Fakultas Hukum Universitas Gadjah Mada* 30, no. 2 (2018): 263. https://doi.org/10.22146/jmh.30855.

Sulistianingsih, Dewi, Miftakhul Ihwan, Andry Setiawan, and Muchammad Shidqon Prabowo. "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-

Undang Perlindungan Data Pribadi)." *Masalah-Masalah Hukum* 52, no. 1 (2023): 98. https://doi.org/10.14710/mmh.52.1.2023.97-106.

Tobing, Michael Yusuf Lumbang, Miquel Joan Markus Aruan, and Kartina Pakpahan. "Penggunaan Big Data Dalam Mengungkap Kasus Kejahatan Judi Online Di Polrestabes Medan." *Journal of Economic and Business Law Review* 3, no. 1 (2023): 1–25. https://doi.org/10.19184/jeblr.v3i1.24445.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Windani, Cynthia Ayu. "Strategi Dan Tantangan Predictive Policing Di Era Big Data Bagi Masyarakat Modern." *Deviance Jurnal Kriminologi* 7, no. 2 (2023): 101–20. https://doi.org/10.36080/djk.2385.

Zarsky, Tal. "The Trouble with Algorithmic Decisions." *Science, Technology, & Law*, 14, no. 1 (2016): 45–78. https://doi.org/10.2139/ssrn.2687057

DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no conflict of interest in the publication of this article.

FUNDING INFORMATION

None

ACKNOWLEDGMENT

None

HISTORY OF ARTICLE

Submitted : January 22, 2025
Revised : December 6, 2025
Accepted : November 4, 2025
Published : December 18, 2025