Sophist: Jurnal Sosial Politik, Kajian Islam dan Tafsir
Vol. 8, No. 3, 2026
Published by Fakultas Ushuluddin dan Studi Agama (FUSA), UIN Mataram
p-ISSN 2656-1220, e-ISSN 2745-8571, available online at https://sophist.or.id

PERSONAL DATA PROTECTION IN ARTIFICIAL INTELLIGENCE-BASED LAW ENFORCEMENT FROM A HUMAN RIGHTS PERSPECTIVE

Dian Dwi Pratiwi, Tiara Dhiya Nafisah, Septiyan Dwi Putra, Asep Suherman

Faculty of Law, University of Bengkulu

diandwipratiwi47@gmail.com, tiaradhiya709@gmail.com, riyn.septiyan88@gmail.com, asepsuherman@unib.ac.id

Abstract: The use of Artificial Intelligence in law enforcement enhances data processing and analysis capabilities but also creates risks to personal data protection and the right to privacy. This research addresses the gap between legal guarantees for personal data protection and actual data processing practices in AI-driven law enforcement, along with the need to strengthen that protection from a human rights perspective. The study analyzes problems in personal data protection within AI-driven law enforcement and proposes measures to strengthen that protection and safeguard the right to privacy. It uses a normative-juridical method, drawing on statutory and conceptual approaches. The findings show that Law Number 27 of 2022 on Personal Data Protection provides a legal foundation but does not yet fully address the specific characteristics of data processing in AI-driven law enforcement. Strengthening that protection calls for risk-based regulation, limits on data purposes and access, human rights impact assessments, privacy by design, transparency, independent oversight, human oversight, and effective redress mechanisms. The use of Artificial Intelligence in law enforcement must therefore remain consistent with the principles of legality, necessity, proportionality, and respect for the right to privacy.

Keywords: Artificial Intelligence, Personal Data, Privacy, Human Rights, Law Enforcement

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

INTRODUCTION

Digital technology, particularly artificial intelligence (AI), has changed many fields, including law enforcement. AI lets agencies process and analyze large volumes of data to support decision-making. But that same capability increases the collection and processing of personal data, which puts the right to privacy at risk. Personal data has become central to technological development, yet its use needs adequate legal protection to prevent misuse. (Rahman, 2021)

From a human rights perspective, the right to privacy is a fundamental right attached to every individual, tied to personal dignity and freedom. Personal data protection forms part of that right because individuals have an interest in controlling information about themselves and deciding who may access or use it. (Kusnadi, 2021) As governments and private actors collect, use, and share more data, the need for that protection keeps growing. (Claudia & Sitaboeana, 2021)

Digitalization also brings the risk of data loss, damage, theft, and leaks. When personal data reaches unauthorized parties, individuals lose control over their own information, which can violate their right to privacy. At its core, privacy gives people the ability to set limits on what others can know or access about them. (Djafar et al., 2015, p. 32) Personal data protection therefore is not just a matter of technological security; it is also part of respecting human rights. (Koirunisyah et al., 2026, p. 3)

The right to privacy has constitutional backing under Article 28G(1) of the 1945 Constitution, which protects a person's self, honor, dignity, family, and property. Law No. 39 of 1999 on Human Rights and Law No. 27 of 2022 on Personal Data Protection (the PDP Law) reinforce that protection. Personal data protection also connects to Law No. 1 of 2024 on the Second Amendment to the Electronic Information and Transactions Law. The right to privacy is likewise recognized under Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). (Argiansyah & Prawira, 2024)

As duty bearer, the state must respect, protect, and fulfill human rights, including the right to privacy and personal data protection. Yuli Asmini, Mengembangkan Indikator Hak Asasi Manusia: Sebuah Pengalaman Komnas

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

HAM, Jakarta: Komnas HAM, 2014, p. 3. Even so, several data breach cases show that this protection has not worked effectively in practice. Notable cases include the alleged data breaches at BPJS Ketenagakerjaan, Bank Syariah Indonesia, and Indonesian citizens' passport data. (RDS, 2023) This reveals a persistent gap between the das sollen, the legal guarantee of privacy and data protection, and the das sein, the continued occurrence of data breaches and misuse.

This problem becomes more complex when AI is used in law enforcement, because the technology requires collecting, processing, and analyzing data on a large scale. Large-scale data use raises questions about the limits of data collection, the purpose of processing, storage security, third-party access, and accountability when misuse occurs. Rahman argues that technologies such as big data and AI need a legal framework that balances the state's interest in using data with individuals' interest in privacy and information security. (Rahman, 2021)

Indonesia already has Law No. 27 of 2022 on Personal Data Protection as the specific legal basis for personal data protection. Its implementation, however, still faces various problems, including oversight, enforcement, and the need to keep regulation current with advances in AI technology. (Koirunisyah et al., 2026) The question worth examining, then, is not just whether rules exist, but how far those rules actually protect the right to privacy in AI-based law enforcement practice.

Based on this background, the research questions this study addresses are why personal data protection in AI-based law enforcement still faces problems from a human rights perspective, and how that protection can be strengthened to safeguard the right to privacy. This discussion matters for assessing whether the growing use of AI, the applicable legal provisions, and the state's obligations to protect privacy as a human right actually fit together.

METHOD

This study uses a normative-juridical method, examining positive legal norms and the doctrines that have developed within legal scholarship. It applies a statute approach, analyzing provisions on the right to privacy and personal data protection, particularly Law No. 27 of 2022 on Personal Data Protection as the primary legal basis. It also applies a conceptual approach, drawing on scholarly views and doctrines concerning the right to privacy,

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

personal data protection, human rights, individual autonomy, and human dignity.

The legal materials used consist of primary and secondary sources. Primary sources are the relevant statutes, particularly Law No. 27 of 2022 on Personal Data Protection and other regulations concerning privacy and human rights. Secondary sources are relevant books and legal literature, including Peter Mahmud Marzuki's work on legal research methods and legal reasoning theory, which underpins the normative analysis. (Marzuki, 2017, pp. 133–137) All legal materials are analyzed qualitatively through legal interpretation and deductive reasoning to arrive at prescriptive, argumentative conclusions.

RESULTS AND DISCUSSION

Looking at privacy, it should not be understood narrowly as a purely private matter; it is a precondition for exercising other human rights. Warren and Brandeis (1890) first framed it as the right to be let alone, meaning protection of the individual from others' interference in their private life. (Myers, 2020) Subsequent scholarship showed that privacy is not a single concept, but covers a range of interests, including how information about a person is collected, processed, and disseminated. This broadened meaning is what turns personal data protection into privacy's contemporary form.

In the digital era, threats to privacy go beyond physical intrusion or the exposure of secrets; they now include large-scale data collection and analysis that can build a complete picture of a person without their knowledge. This shift is what drove the emergence of personal data protection regimes at the international, regional, and national levels.

Under international human rights law, the right to privacy is guaranteed by Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which prohibits arbitrary or unlawful

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

interference with a person's private life, family, home, and correspondence. (International Covenant on Civil and Political Rights [ICCPR], 1966) Indonesia is bound by this provision through Law No. 12 of 2005 ratifying the ICCPR. The UN Human Rights Committee, in General Comment No. 16 (1988), interpreted this to mean that public authorities' collection and storage of personal information, whether in computers, data banks, or other devices, must be expressly regulated by law. (Finn & Prescott, 2025) This interpretation matters because it confirms that the right to privacy has long covered personal data, and that state processing of that data needs a clear legal basis rather than mere internal institutional policy.

At the national level, a similar guarantee appears in several layers. Article 28G(1) of the 1945 Constitution grants everyone the right to protection of their person, family, honor, dignity, and property, and the right to feel secure from the threat of fear to do or not do something that is a basic right. (1945 Constitution of the Republic of Indonesia, art. 28G(1)) This is elaborated in Article 29(1) of Law No. 39 of 1999 on Human Rights, which guarantees the right to protection of one's person, family, honor, dignity, and property. (Law No. 39 of 1999, art. 29(1)) Together, these provisions show that Indonesian law treats personal data protection as part of protecting a person's dignity and integrity, meaning violations are not just an administrative problem but a human rights one.

That said, the right to privacy is not absolute, and this discussion needs to place proportional limits on it. Article 28J(2) of the 1945 Constitution and Article 73 of Law No. 39 of 1999 allow restrictions on rights and freedoms, but only through legislation and for specific purposes: securing recognition and respect for the rights of others, and

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

meeting the just demands of morality, religious values, security, and public order in a democratic society. (Suari & Sarjana, 2023)

Under international law, the Siracusa Principles spell out the conditions for such restrictions: they must be prescribed by law, pursue a legitimate aim, and be necessary and proportionate in a democratic society. The Office of the UN High Commissioner for Human Rights has reinforced this reading in the context of digital technology, stating in its reports that surveillance and data collection must meet the necessity and proportionality tests, and that mass data collection without specific suspicion struggles to meet that bar.

These three conditions are the yardstick for this entire discussion. The first, legality, requires that any restriction be set out in legislation clear enough for citizens to foresee its consequences. The second, legitimate aim, requires that the restriction serve a recognized interest, such as law enforcement or security, rather than an arbitrary or unrelated purpose. The third, necessity and proportionality, requires that the restrictive measure actually be needed to achieve that aim and go no further than necessary. By this standard, the use of technology in law enforcement, including AI-based technology, should be judged not just by how effective it is, but by whether it stays within the limits set by human rights law.

The most basic problem in personal data protection within AI-based law enforcement lies in how Law No. 27 of 2022 on Personal Data Protection (the PDP Law) treats law enforcement interests. Article 15(1) exempts a number of data subject rights when processing serves specific purposes: national defense and security, law enforcement, the public interest in state administration, and oversight

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

of the financial services, monetary, payment system, and financial system stability sectors. (Law No. 27 of 2022, art. 15(1)) Article 15(2) then states that this exemption applies only within the bounds of statutory implementation. Exemptions of this kind are, in principle, common in data protection regimes, because the state does need room to prevent and act against crime. The issue is not whether an exemption exists, but how clearly its limits are drawn.

The UN Human Rights Committee, in General Comment No. 16 (1988), states that public authorities' collection and storage of personal data must be expressly regulated by law. Without that detail, law enforcement's authority to process data becomes extremely broad, while citizens cannot predict when or how their data will be processed. That makes it hard to test whether a given instance of processing meets the necessity and proportionality requirement, as the Office of the UN High Commissioner for Human Rights has stressed. (Fitri, 2022)

This gap in detail is felt even more because the PDP Law was never designed as a dedicated instrument for data processing by law enforcement officials. It functions as a general umbrella statute covering data controllers across individuals, public bodies, and organizations, so its provisions are written in general terms. (Jyoti, 2025) That general framing falls short of addressing the distinct character of data processing in law enforcement: coercive authority, a direct impact on individual freedom, and a high potential for abuse.

This weakness is rooted in the sectoral history of personal data regulation in Indonesia. Scholarship shows that before the PDP Law, rules on personal data were scattered across various sectoral statutes, covering telecommunications, population administration, banking, and health, each with different, uncoordinated standards. Related work

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

likewise notes that personal data protection in Indonesia had long been handled piecemeal through separate regulations, which never delivered full legal certainty. As a result, data processing by law enforcement has no strict standard of its own. In practice, officials rely on authority drawn from each institution's own sectoral statute, while the PDP Law supplies only general principles and exemptions. This absence of a dedicated standard leaves oversight of law enforcement's data processing dependent on each institution's internal mechanisms rather than on a uniform data-protection norm.

The Constitutional Court's position in Decision No. 20/PUU-XIV/2016 confirms that the legality requirement for restricting privacy is already recognized in Indonesian law. (Sanjaya, 2022) In that decision, the Court held that wiretapping, as a form of privacy restriction, must be regulated by statute to prevent abuse of authority. The same logic can, and should, apply to AI-based data collection and processing, since the technology can gather and analyze personal information on a scale far beyond conventional wiretapping. The decision implies that restrictions on privacy by law enforcement cannot rest on internal policy; they need an explicit, measurable legal basis.

Looking at the European Union's 27 member states offers a useful comparison, since they face the same question: how a state can use data and technology for law enforcement without sacrificing the right to privacy. (Al Qatawneh et al., 2022) There, the right to private life and the right to personal data protection are recognized separately, under Articles 7 and 8 of the EU Charter of Fundamental Rights. This comparison is not meant to replicate the European model wholesale, since Indonesia is not bound by the European Convention on Human

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

Rights or EU law. Rather, European decisions and regulations are discussed as comparative reference points, showing how another jurisdiction translates the legality, necessity, and proportionality requirements into operational norms.

The first lesson concerns regulatory structure. The General Data Protection Regulation (GDPR) does not apply to data processing by competent authorities for preventing, investigating, detecting, or prosecuting criminal offenses. That area is governed separately by Directive (EU) 2016/680, drafted in line with the GDPR but adapted to law enforcement's distinct character. The Directive also requires distinguishing between categories of data subjects, such as suspects, convicted persons, victims, and third parties, so that someone who is not a suspect is not treated the same as an offender. It also contains specific rules on decisions based solely on automated processing, including profiling, which are prohibited by default unless authorized by law with adequate safeguards. (De Hert & Sajfert, 2024)

The second lesson comes from human rights case law, particularly the European Court of Human Rights' decision in S. and Marper v. the United Kingdom (2008). This ruling matters for the AI discussion because the technology works by gathering and matching data at scale. The larger the biometric database held by law enforcement, the greater the risk that innocent people end up stored and processed without limit. The message for Indonesia is clear: the necessity and proportionality requirement demands differentiation, time limits, and periodic review, not just the existence of a legal basis. (Sabila & Widiyawati, 2025)

The third lesson comes from a recent development: Regulation (EU) 2024/1689, the AI Act, which regulates AI through a risk-based

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

approach. AI systems are grouped by risk level, from those banned for posing unacceptable risk, through high-risk systems subject to strict obligations, down to low-risk systems with limited obligations. (Vaddiparti & Babaiev, 2025) Such use is prohibited in principle and only exempted for very narrow purposes, such as searching for specific victims, preventing a specific, serious, and imminent threat, or locating suspects of certain serious crimes, and only with prior authorization from a judicial or independent administrative authority and an assessment of the impact on fundamental rights.

The discussion so far shows that the problem of personal data protection in AI-based law enforcement is systemic. Broad exemptions, the absence of dedicated norms, the risk of bias, oversight that is not yet independent, and weak redress all reinforce one another. Strengthening protection therefore cannot rest on a single instrument or institution. The UN General Assembly, in Resolution 73/179 (2018), called on states to align their national laws with human rights obligations in the digital age, including guaranteeing transparency, accountability, and effective redress for data processing by both the state and private actors. That call can be translated into four layers of strengthening that need to move together: norms, technology, institutions, and redress. (Triadi & Cahyono, 2025) All four are designed so that the three conditions for restricting rights that serve as this discussion's yardstick, namely legality, legitimate aim, and necessity and proportionality, can actually be tested in practice.

1. Strengthening Norms in the PDP Law

Strengthening at the norm level starts with issuing implementing regulations that close the detail gap in Law No. 27 of

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

2022 on Personal Data Protection (the PDP Law). Those regulations need to set operational limits on data processing by law enforcement: specific processing purposes, the categories of data that may be collected, retention periods, an obligation to delete data no longer needed, and a ban on using data for unrelated purposes.

Strengthening the norms should also narrow Article 15 of the PDP Law. The law enforcement exemption should not be left as a blanket exception; it needs to be tied to testable conditions, such as a specific legal basis, a clear purpose, authorization matched to the type of action, and oversight of its implementation. This approach lines up with the legality requirement in the Siracusa Principles and with the Constitutional Court's position in Decision No. 20/PUU-XIV/2016, which held that restrictions on privacy must be set by statute. (Warouw, 2025) Beyond that, dedicated rules on AI and biometrics in law enforcement are needed. These should cover biometric surveillance such as facial recognition, a transparency obligation for law enforcement's use of AI systems, and the right to request human review of decisions based on automated processing.

2. Strengthening the Technology Dimension

At the technology level, protection needs to be built in from the start, not bolted on after a system is already running. The privacy-by-design principle requires that purpose limitation, data minimization, and security become part of an AI system's architecture from the outset, as Directive (EU) 2016/680 also provides. Indonesia already has a normative basis for this in the data protection impact assessment obligation for high-risk processing under Article 34 of the PDP Law. That obligation should ideally be expanded into a human rights impact assessment before law

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

enforcement deploys any AI system, since the risks involved go beyond data leaks to include discrimination, restrictions on freedom, and due process violations.

The technology dimension also involves private providers. AI systems for law enforcement are often developed, sold, or managed by technology companies, so human rights protection cannot rest on law enforcement alone. The UN Guiding Principles on Business and Human Rights affirm companies' responsibility to respect human rights through due diligence, alongside the state's duty to protect. In this context, public procurement of technology can serve as an entry point, for example by requiring impact assessments, independent audits, and transparency guarantees as contract preconditions. (Girsang, 2024)

3. Strengthening Institutions

At the institutional level, strengthening centers on an independent, empowered supervisory body. Article 58 of the PDP Law provides that the personal data protection authority is appointed by, and accountable to, the President, which raises questions about its independence when the entity being supervised is itself a state institution. Comparative literature stresses that a data protection regime's effectiveness depends heavily on having a strong, autonomous supervisory authority with real powers. That authority needs the power to assess compliance by public bodies, including the police and prosecutors, inspect the AI systems they use, receive complaints, and impose binding sanctions or recommendations. Adequate staffing and budget also matter, since overseeing technical systems demands real competence.

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

Involving national human rights institutions can strengthen this oversight. The Paris Principles affirm the role of independent national human rights institutions in monitoring and advancing human rights. In Indonesia, Komnas HAM (the National Commission on Human Rights) holds a mandate to promote and monitor human rights under Law No. 39 of 1999. Its involvement, for instance through coordination or input into impact assessments and complaint handling, helps ensure that human rights standards, not just administrative compliance, factor into how law enforcement's use of AI is evaluated. The establishment status and authority of the personal data protection authority should be verified against the latest information before this manuscript is submitted.

The Right to Privacy as a Constitutional Limit on the Use of Artificial Intelligence

Using Artificial Intelligence (AI) in law enforcement lets officials apply the technology for a wide range of purposes, from biometric identification, surveillance, and digital evidence analysis to pattern recognition, profiling, and predicting potential risk. This capability grows more complex because AI can process and link data from multiple sources to generate new information about a person. That creates a distinct privacy problem, since the information produced this way may never have been disclosed or even known directly by the individual concerned. The threat to privacy in AI use therefore comes not only from possible data leaks, but also from excessive data collection, using data beyond its original purpose, errors in identification, and labeling someone as a risk without adequate individual assessment. (Casaburo & Marsh, 2024)

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

This issue becomes even more important once AI output is used as part of the law enforcement process. Inaccuracy, incompleteness, or bias in the underlying data can skew the analysis and lead to a flawed assessment of a person. As a result, someone can end up treated as a suspect or categorized at a certain risk level despite having no actual connection to the crime being investigated. This shows that applying AI in law enforcement cannot be judged only by how much it speeds up or streamlines the work of officials; it must also account for its consequences on a person's legal standing, privacy, and rights.

From a human rights perspective, a state action that touches on privacy is not automatically justified just because it aims to prevent or uncover crime. Every form of intervention still needs a clear legal basis, a legitimate purpose, genuine necessity, and proportionate implementation. The proportionality principle matters especially in AI use, because overly broad or uncontrolled deployment can affect other rights too, such as freedom of expression, equality, the presumption of innocence, and the right to a fair trial. (Casaburo & Marsh, 2024)

The wider AI's ability to access, link, and process different kinds of information becomes, the greater the chance that state surveillance over individuals will expand too. AI's use in law enforcement therefore needs to stay within clear, accountable limits. Using the technology should not rest merely on the fact that it is available or can boost efficiency; it needs real necessity tied to achieving a law enforcement objective. Its application should also

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

consider whether another approach could reach the same goal with less risk or impact on individual rights.

Beyond that, AI-generated analysis should not be used directly as the basis for deciding a person's legal treatment. Algorithmic errors, data limitations, and bias built into a system can all skew the analysis and risk producing a decision that harms the individual. Any AI output that can affect someone's rights therefore needs human review and reassessment. That oversight cannot be a mere formality; it must give officials room to check the data's accuracy, understand the case context, and weigh the reasoning behind the system's output. AI then stays in its proper place as a tool that assists law enforcement, while decisions that carry implications for individual rights remain a human responsibility.

The PDP Law Framework and Regulatory Gaps in AI Use

Law No. 27 of 2022 on Personal Data Protection (the PDP Law) provides the legal foundation for personal data protection through provisions on data subject rights, the obligations of data controllers and processors, data processing principles, and forms of accountability in handling data. These provisions are also relevant to technology-assisted decision-making, particularly through Article 10 of the PDP Law, which gives data subjects the right to object when a decision is based solely on automated processing and produces a legal effect or significantly affects them. This shows that Indonesian law does not treat technology use as a process entirely free of oversight; it still leaves room for individuals to assert their rights when an automated decision affects their legal standing.

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

However, these general provisions do not fully resolve the problems in using AI for law enforcement. More operational rules are still needed on algorithmic transparency, system audits, human rights impact assessments, data quality, and clear accountability when AI output causes harm to an individual. More detailed regulation is needed so that AI use rests not only on legal authority, but can also be supervised and held accountable when it affects someone's rights. (Kurdi & Cahyono, 2024) The problem, then, is not the absence of a legal basis for data protection in Indonesia, but a persistent gap between general regulation and the governance that AI, with its more complex risks to individual rights, actually needs.

This gap shows up in several important aspects of AI use in law enforcement that remain unintegrated: data access limits, processing purposes, data sources and quality, retention periods, system testing, independent oversight, and objection and correction mechanisms. Yet these are exactly the elements that make AI use accountable when its output affects someone's rights. Data protection in Indonesia therefore needs strengthening through regulatory harmonization, technical guidelines, stronger institutional capacity, and effective oversight, so that it does not stop at normative rules but is actually implemented in practice. (Purnomo, 2026)

A Model for Strengthening Personal Data Protection in AI-Based Law Enforcement

Based on this study, strengthening personal data protection in AI use for law enforcement should move toward governance that not only safeguards data security but also weighs the technology's potential human rights impact throughout its use. That governance

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

can include risk-based regulation, human rights impact assessment, data management built in from the system design stage, transparency in AI use, independent oversight, and stronger competence among the officials who operate it.

1. Dedicated Risk- and Purpose-Based Regulation

AI use in law enforcement needs to be differentiated by risk level and its impact on individual rights, since each type of use carries different consequences. Using AI for administrative tasks poses a markedly different risk than remote biometric identification, predictive profiling, or systems that support decisions capable of affecting a person's freedom. The greater the impact on individual rights, the stricter the regulation and oversight should be.

AI use that carries a high human rights risk needs stricter conditions attached: a clear legal basis, a specific purpose, and proof that the use is genuinely necessary and proportionate. Data access and storage must also be limited, and data may not be used for other purposes without an appropriate legal basis. Before deploying such technology, officials should also weigh simpler alternatives that interfere less with individual rights. AI use should rest on real necessity, not simply on the perception that the technology is more efficient. (Kirana & Silalahi, 2025)

A risk-based approach lets the form of oversight scale with the impact level of the technology used. The greater AI's potential to affect someone's freedom or legal standing, the stricter the requirements and oversight should be. This approach fits better because different AI applications carry different capabilities and

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

risks, so treating every deployment under the same standard would not be appropriate.

2. Impact Assessment Before and Throughout the AI Life Cycle

An impact assessment on data protection and human rights should be carried out before any AI system is deployed in law enforcement. It needs to cover the types of data used, who could be affected, the processing purpose, the likelihood and severity of risk, mitigation steps, and who is responsible. The assessment also needs to be repeated periodically, not just at procurement, since risk can shift whenever the model, data sources, intended use, or the system's operating conditions change. (Pei, 2025)

Impact assessments should therefore continue at regular intervals for as long as the AI system is in use. Any change that could raise the risk level should trigger a fresh review. The assessment results also need to be documented, forming the basis for deciding whether the system can keep running, needs fixing, or should be shut down.

An impact assessment should not become a mere administrative document used to justify a decision already made. Its findings need to genuinely shape which technology is chosen and how it is deployed. If the risk to individual rights stays high and cannot be reduced through adequate mitigation, the system's use should be restricted or stopped. Done this way, the impact assessment works as a preventive safeguard for individual rights, not just a box to tick.

3. Data Governance and Privacy by Design

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

Data protection needs attention from the system-design stage of an AI system onward, through data minimization, purpose limitation, role-based access control, access logging, data security and encryption, data segregation, and scheduled deletion. Data quality, accuracy, and representativeness also need regular testing, since AI output depends heavily on the quality of the data feeding the system.

Data protection requirements need to be stronger when a system processes biometric or other sensitive personal data. When AI is procured from a third party, the procurement contract should also clearly set out security obligations, audit access, logging of any change to the system or model, and the division of responsibility between the provider and the using agency. These terms matter for keeping AI use supervisable and accountable.

This governance matters because problems in AI use do not only arise at the moment a system produces a decision. Errors can also originate in data that was inaccurate, incomplete, or unrepresentative of the population from the start. Data protection therefore cannot begin only after data is collected; it needs to apply from collection and selection through storage, processing, and eventual deletion.

Synthesis: Strengthening Personal Data Protection from a Human Rights Perspective

Taken together, these findings show that strengthening personal data protection in AI-based law enforcement cannot rest on data security alone. What matters more is ensuring that every act of accessing, linking, analyzing, and using data has a legal basis, a clear purpose, and real accountability.

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

In law enforcement, the basis for processing data comes essentially from legal authority and the needs of carrying out official duties, not primarily from individual consent as is typical in consumer services. Data processing therefore needs to be assessed against a legitimate purpose, a clear necessity, proportionate use, and the existence of oversight and redress mechanisms for anyone harmed. A law enforcement purpose cannot, by itself, justify every form of intervention into privacy. (Brewczyńska, 2023)

This approach matters because AI can generate new information or inferences from data that was lawfully obtained in the first place. Data collected for one purpose can be combined with other sources until it builds a profile of someone that the person never directly provided or even knew existed. Data protection therefore needs to cover downstream use, data quality, limits on the inference process, and documentation of decisions, not just whether the data was lawfully obtained to begin with.

A human rights impact assessment before deploying AI matters because it helps prevent harm that is hard to undo. Risks such as mass surveillance, discrimination, or errors in automated decisions can do wide damage if they only come to light after the harm has occurred. Impact assessment therefore needs to be part of the decision-making process from the outset. If a system's risk is too high and cannot be adequately reduced, its use should be tightly restricted or not adopted at all.

Protection consistent with a human rights perspective therefore requires AI governance that includes risk-based regulation, limits on purpose and access, impact assessment before

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

and during use, privacy by design, human oversight, transparency, independent audits, and effective redress mechanisms. AI's success in law enforcement should not be measured only by speed or data-processing power, but also by legality, accuracy, proportionality, non-discrimination, and whether individuals have a real chance to correct or object to a decision that affects them. (Srivastav, 2025)

Seen this way, personal data protection should not be viewed as an obstacle to law enforcement, but as a boundary keeping technology use consistent with legal provisions and human rights principles. AI can help officials detect and uncover crime more effectively, but responsibility for decisions and their legal consequences still rests with the people and institutions using the technology. These findings point to the need for stronger normative regulation; gauging how far that plays out in each institution's actual practice is a question for future empirical research using primary data.

CONCLUSION

Based on this discussion, Artificial Intelligence in law enforcement can be concluded to offer real benefits in processing and analyzing data, while also creating risks for personal data protection and the right to privacy. Law No. 27 of 2022 on Personal Data Protection provides a legal basis for personal data protection, but its provisions do not yet fully address the specific characteristics and risks of data processing in AI-based law enforcement. This points to a need to ensure that technology use continues to follow the principles of legality, necessity, proportionality, and respect for human rights.

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

Strengthening personal data protection in AI-based law enforcement calls for risk-based regulation, limits on the purpose and access to data, human rights impact assessment, privacy by design, transparency, independent oversight, and human control over decision-making. An effective redress mechanism is also needed for individuals whose rights are harmed. The advance of AI technology in law enforcement, in short, must be matched by adequate legal protection, so that gains in enforcement effectiveness do not come at the expense of the right to privacy and personal data protection.

The government needs to strengthen regulation of Artificial Intelligence in law enforcement, calibrating it to the risks of personal data processing and the protection of the right to privacy. Law enforcement officials also need to apply limits on data access and use, conduct human rights impact assessments, maintain transparency, and ensure effective oversight. In addition, there needs to be a clear complaint and redress mechanism for individuals harmed by AI use, along with human control over every decision, so that technology use stays aligned with the principles of legality, proportionality, and respect for human rights.

REFERENCES

Casaburo, Donatella, dan Irina Marsh. "Ensuring Fundamental Rights Compliance and Trustworthiness of Law Enforcement AI Systems: The ALIGNER Fundamental Rights Impact Assessment." *AI and Ethics* 4, no. 4 (2024): 1569–1582. https://doi.org/10.1007/s43681-024-00560-0.

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

Claudia, Jennifer, dan Toendjoeng Herning Sitaboeana. "Analisis Hak Privasi Perlindungan Data Pribadi Masyarakat Di Indonesia." *Jurnal Hukum Adigama* 4, no. 2 (2021). https://doi.org/10.24912/Adigama.V4i2.17138.

De Hert, Paul, dan Juraj Sajfert. "Variety, Velocity and Volume of Personal Data in Criminal Investigations and Proceedings: The Limits Drawn by the Purpose Limitation and Data Minimization Principles in Directive (EU) 2016/680." Dalam *Research Handbook on EU Criminal Law*, 212–228. Edward Elgar Publishing, 2024. https://doi.org/10.4337/9781800886438.00017.

Djafar, Wahyudi, et al. *Privasi 101: Panduan Memahami Privasi, Perlindungan Data dan Surveilans Komunikasi*. Jakarta: ELSAM, 2015.

Finn, Tobias, dan Silas Boone Prescott. "The Impact of International Human Rights Law on Digital Privacy in the Era of Mass Surveillance." *Law and Justice Research Journal* 1, no. 1 (2025): 29–35. https://doi.org/10.70062/ljrj.v1i1.36.

Fitri, Okta Rina. "Hak Atas Pelindungan Data Pribadi Pada Proses Penegakan Hukum Pidana." *Jurnal Hak Asasi Manusia* 15, no. 1 (2022): 91–108.

Girsang, Sarimah Yemima Br. "Pentingnya Regulasi Khusus Sistem *Face Recognition Technology* sebagai Produk *Artificial Intelligence* dalam Peningkatan Keamanan dan Penegakan Hukum di Indonesia." *Nommensen Journal of Legal Opinion* (2024): 86–98. https://doi.org/10.51622/njlo.v5i2.1817.

International Covenant on Civil and Political Rights (ICCPR).

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

Jyoti, Jyoti. "Impact of the Digital Personal Data Protection Act on Law-Enforcement Investigations." *LawFoyer International Journal of Doctrinal Legal Research* 3, no. 4 (2025): 1267–1287.

Kirana, Kimmy Baby, dan Wilma Silalahi. "Tantangan Regulasi Kecerdasan Buatan (AI) Dalam Perspektif Hukum Perlindungan Data Pribadi Di Indonesia." *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 6 (2025): 1807–1817. https://doi.org/10.59141/cerdika.v5i6.2711.

Koirunisyah, Prasasti Pelangi, Mufidatus Sholeha, Althaf Misbahuddin Iqbal Nurdiyanto, Putry Zulkarnaini Sarkasi, dan Selly Rizki Rahmawati. "Urgensi Regulasi Perlindungan Data Pribadi pada Penegakan Hukum Berbasis Artificial Intelligence dalam Perspektif HAM." *Jurnal Media Akademik (JMA)* 4, no. 7 (2026). https://doi.org/10.62281/r4fays91.

Kusnadi, Sekaring Ayumeida. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *Al Wasath Jurnal Ilmu Hukum* 2, no. 1 (2021). https://doi.org/10.47776/Alwasath.V2i1.127.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Edisi Revisi. Jakarta: Kencana Prenada Media Group, 2017.

Myers, Cayce. "Warren, Samuel & Louis Brandeis. The Right to Privacy, 4 Harv. L. Rev. 193 (1890)." *Communication Law and Policy* 25, no. 4 (2020): 519–522.

Purnomo, Hadi. "Personal Data Protection in Indonesia's Digital Law Enforcement System." *AKSELERASI: Jurnal Ilmiah Nasional* 8, no. 1 (2026): 118–125. https://doi.org/10.54783/jin.v8i1.1762.

Rahman, Faiz. "Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

Indonesia." *Jurnal Legislasi Indonesia* 18, no. 1 (2021): 81–102. https://doi.org/10.54629/jli.v18i1.736.

RDS. "Deret Insiden Kebocoran Data WNI 2023, BPJS Hingga Dukcapil." *CNN Indonesia*, 19 Juli 2023. Diakses 10 Oktober 2026.

Sabila, Silvina Viola, dan Anis Widiyawati. "Use of AI Risk Assessment for Conditional Release Based on Principles of Justice and Protection of Human Rights." *Jurnal Daulat Hukum* 8, no. 4 (2025): 986. https://doi.org/10.30659/jdh.v8i4.49971.

Sanjaya, Aditya Wiguna. "Anotasi Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016." *Jurnal Magister Hukum Perspektif* 12, no. 1 (2022): 39–53. https://doi.org/10.37303/magister.v12i1.56.

Suari, Kadek Rima Anggen, dan I Made Sarjana. "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia." *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–142.

Triadi, Irwan, dan Marsha Putri Cahyono. "Hukum Internasional Dalam Perlindungan Hak Asasi Manusia Di Era Digital." *Birokrasi: Jurnal Ilmu Hukum dan Tata Negara* 3, no. 1 (2025): 85–93. https://doi.org/10.55606/birokrasi.v3i1.1829.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

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

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

Vaddiparti, Surya Sagar, dan Fuad Babaiev. "Balancing Public Safety and Civil Rights: Successes and Challenges of AI-Based Video Surveillance Systems." *Law. Human. Environment* (2025): 118–134. https://doi.org/10.31548/law/2.2025.118.

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.

Viola, M. Brewczyńska. "Between Legitimacy and Lawfulness: In Search of Rationality and Consistency in EU Data Protection." *European Data Protection Law Review* 9, no. 2 (2023): 112–122. https://doi.org/10.21552/edpl/2023/2/6.

Warouw, Ahmad Sauki. "Peran Hukum Pidana Dalam Perlindungan Data Pribadi Dan Pencegahan Kejahatan Siber Di Indonesia." *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora* 2, no. 6 (2025): 65–71. https://doi.org/10.62383/aliansi.v2i6.1310.

Yemima, Sarimah Br Girsang. "Pentingnya Regulasi Khusus Sistem *Face Recognition Technology* sebagai Produk Artificial Intelligence dalam Peningkatan Keamanan dan Penegakan Hukum di Indonesia." *Nommensen Journal of Legal Opinion* (2024): 86–98. https://doi.org/10.51622/njlo.v5i2.1817.

© 2026 The Author(s). Published by Sophist: Jurnal Sosial Politik Kajian Islam dan Tafsir, Faculty of Ushuluddin and Religious Studies, Universitas Islam Negeri Mataram. This is an open access article under the CC BY-SA 4.0 license.