

Human Rights Law in the Big Data Era: Islamic IR Perspective and Maqashid Syari'ah Approach

Devi Aghita Arifani¹ and Calya Maharani²

^{1,2} Humanities, University of Darussalam Gontor, Ngawi, Indonesia

*Corresponding author: deviaghita02arifani@gmail.com

ABSTRACT

The rapid advancement of big data has created a paradox in the field of human rights enforcement, it offers powerful tools for documentation and transparency, while simultaneously posing serious risks to privacy, justice, and digital freedom. However, limited scholarly attention has been given to how Islamic ethical frameworks can guide the governance of big data in global conflict contexts. This study addresses that gap by asking: To what extent can Islamic International Relations (IR), particularly the principles of Maqashid al-Shari'ah, offer an ethical response to the misuse of big data in human rights violations?. Using a qualitative descriptive method and case study analysis, this paper explores the intersection between human rights law, the use of big data in conflict zones (e.g., Palestine-Israel), and Islamic ethical theory. The findings show that while big data has the potential to support justice and accountability through fast, verifiable digital evidence, it also reinforces digital inequality and surveillance when misused by powerful actors. From an Islamic perspective, principles like ḥifẓ al-naḥs (protection of life) and 'adālah (justice) can serve as moral compasses to guide ethical data governance and challenge the digital power imbalance. This study suggests that integrating Islamic values into digital policy and international law can strengthen human-centered technology and promote equitable global data governance.

Keywords: Big Data, Human Rights, Islamic International Relations, Maqashid al Shari'ah, Digital Ethics, Justice, Surveillance

1. INTRODUCTION

Human rights are universal principles that guarantee the freedom, dignity, and basic rights of every individual without discrimination. Since the adoption of the Universal Declaration of Human Rights (UDHR) in 1948, these principles have become the normative foundation for both international and national legal systems. However, in the era of digital transformation, particularly with the rise of big data technologies. New challenges have emerged that threaten the realization of these rights. Big data offers immense capabilities for collecting, analyzing, and predicting human behavior. While this can enhance public services and policy-making, it also opens the door to mass surveillance, algorithmic discrimination, and misuse of personal data, especially when governance and ethical standards are weak. This paper is motivated by the growing tension between technological advancement and the protection of human rights, particularly in conflict zones and authoritarian settings. Globally, digital tools are increasingly used not only for social good but also for control, repression, and asymmetrical warfare. In the Global South including Indonesia. This issue is further complicated by weak digital literacy and underdeveloped regulatory systems, increasing the vulnerability of citizens to rights violations.

From an Islamic perspective, the ethical foundation provided by Maqashid al-Shari'ah offers a valuable framework for rethinking digital governance. The principle of ḥifẓ al-naḥs (protection of life) emphasizes the preservation of human dignity and security, including

protection from digital harm. Similarly, the value of ‘adālah (justice) calls for a fair distribution of information power and accountability in data usage. Islamic International Relations (IR), as an emerging discipline, seeks to bridge global legal norms with Islamic ethical principles offering a unique lens through which digital human rights issues can be addressed. While previous studies have examined the role of big data in governance and its implications for human rights (e.g., surveillance practices, algorithmic injustice), few have explored this issue through the normative lens of Islamic ethics and IR. This paper aims to fill that gap by providing a conceptual analysis that integrates Islamic legal philosophy with current global challenges in data ethics and human rights law. Thus, it contributes not only to the Islamization of international legal discourse but also to the broader academic conversation on digital justice and governance.

Conceptual Framework & Literature Review

Human rights are a set of inherent rights that belong to every individual from birth and cannot be revoked by anyone. In the context of international law, HR have the status of universal norms recognized by the global community through various instruments such as the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), and the International Covenant on Economic, Social and Cultural Rights (1966). (Universal Declaration of Human Rights Preamble, n.d.) The definition of human rights has evolved over time, from a focus on civil and political rights to include economic, social, cultural, and even digital rights in the technological era. According to the 2020 report by the UN Human Rights Office, developments in human rights also touch on contemporary issues such as the right to data protection, freedom in the digital space, and access to technology as part of the right to development. The main principles in human rights law include universality, non-discrimination, interdependence, participation, and accountability. The principle of universality emphasizes that all humans, without exception, are entitled to human rights; while the principle of non-discrimination rejects differential treatment based on race, gender, religion, or social status. (Sofian, n.d.) Interdependence states that all rights are interrelated, for example, the right to education is related to the right to information. Participation refers to the active involvement of individuals in decision-making processes that affect their rights, while accountability requires states to be responsible for human rights violations that occur within their jurisdiction. These principles form the main foundation for public policy development, including the formulation of digital regulations.

The implementation of human rights law is carried out in three main dimensions: the state's obligation to respect, protect, and fulfill these rights. “Respecting” means not directly violating citizens' rights, such as arbitrarily restricting freedom of expression. “Protecting” requires the state to take action against third parties, such as private companies, so that they do not violate human rights. (Baderin, 2010) Meanwhile, “fulfilling” means that the state must take active steps to ensure the fulfillment of rights, for example by building inclusive education or health systems. In the context of the digital age, the state must also ensure that digital transformation does not sacrifice basic rights such as privacy, data security, and freedom of expression. However, the implementation of human rights law often faces significant challenges, especially in developing countries that face a dilemma between economic development and rights protection. For example, countries that encourage digital investment

sometimes neglect the rights of digital workers, such as gig workers on digital platforms, who do not receive social security protection or clarity on their employment status. Furthermore, in the context of data collection and analysis by governments and companies, human rights principles such as informed consent or complaint mechanisms are often not followed. This shows that human rights must be integrated from the planning stage of technology policies, rather than being a secondary consideration.

Global digital transformation also expands the scope of responsibility of states and non-state actors for human rights protection. Actors such as technology companies, internet service providers, and artificial intelligence developers have a significant influence on the fulfillment of human rights, even though they are not state entities. (Ridwan et al., n.d.) Therefore, many international institutions have begun to emphasize the importance of corporate responsibility for human rights through guidelines such as the UN Guiding Principles on Business and Human Rights. In 2022, a report by Business for Social Responsibility highlighted how digital companies need to conduct human rights due diligence in designing and implementing their technology products. This includes ensuring that their algorithms do not discriminate, their platforms do not spread hate speech, and user data is not misused.

Thus, human rights law is not merely an international legal norm, but an ethical framework and public policy that must be continuously updated to remain relevant to the times. In the era of big data, human rights principles must be the basis for designing digital technology and policies. In this context, integrating human rights law into data governance is not only a matter of protection but also of empowerment: how data can be used to strengthen access to basic rights such as education, health, and political participation. With transparent and accountable oversight, the digital era should be a driver for strengthening human rights, not the opposite. Big data is a collection of very large and complex data collected from various sources, such as social media, digital sensors, online transactions, and personal devices. In the context of human rights, big data has been used by states and organizations to predict social needs, improve public services, and detect security threats earlier. For example, during the COVID-19 pandemic, many countries used location-based digital tracking data to monitor citizens' movements and control the spread of the virus. (Zhang, 2018) While this technology has proven effective in terms of public health, it has raised concerns about violations of individual privacy and the misuse of data by the state. This highlights that the function of big data is not neutral; it can either strengthen human rights protection or endanger it, depending on the ethical framework and regulations in place.

However, in practice, the use of big data often poses serious challenges to human rights protection, particularly in the context of digital surveillance, algorithmic discrimination, and lack of transparency in data processing. One of the main challenges is the practice of mass surveillance carried out by the state through facial recognition cameras, communication metadata tracking, or the use of spyware software. Such practices can violate the right to privacy, freedom of expression, and even freedom of movement, as stipulated in the International Covenant on Civil and Political Rights (ICCPR). Recent studies indicate that countries such as China, India, and even some Western nations have used digital data as a tool for social control, not merely for public security. Another challenge arises from the use of socially biased algorithms. When the data used to train artificial intelligence (AI) systems is

biased, the algorithm's results will reproduce social injustice. In many cases, facial recognition systems have lower accuracy for individuals of certain races or genders, leading to misidentification with serious consequences, such as wrongful arrests by law enforcement. (Serangan Israel Berlanjut Di Gaza, Sasar Warga Sipil Dan Infrastruktur - ANTARA News, n.d.) Additionally, large technology companies developing big data systems often do not provide public access to how data is processed and used, which contradicts the principles of accountability and participation in human rights.

Global case studies show that human rights violations in the context of big data are not just hypothetical, but a reality that is currently unfolding. One major case is the Pegasus scandal, in which software created by the NSO Group was used to spy on activists, journalists, and human rights defenders in more than 45 countries. (Muhammadiyah Jakarta & Pendapatan Daerah Provinsi DKI Jakarta, 2023) Their data was collected illegally and used to silence criticism of the government. Investigations by Amnesty International and Forbidden Stories show that the use of advanced technology without adequate oversight has become an effective tool of digital repression. This scandal proves that even though technology is developed in the name of security or efficiency, without human rights controls, it can become a systemic threat to civil liberties. This situation also highlights that the current international legal framework is lagging behind technological advancements. While various international human rights instruments have recognized the right to digital privacy, many countries have not yet regulated the use of big data in their national legislation in detail. (Studi et al., 2018) Even in developed countries, oversight of digital service providers remains weak, allowing them to collect and monetize user data without limits. Therefore, regulatory reforms are needed that integrate human rights principles into the design of digital technology, as well as promote transparency, public participation, and protection for vulnerable groups in the use of big data.

In the context of the Global South, including Indonesia, ethical challenges in the use of big data are increasingly complex due to weak legal infrastructure and low digital literacy among the public. The Indonesian government, for example, has used tracking systems such as PeduliLindungi during the pandemic, but regulations on the management of such data remain questionable. A report from SAFEnet (Southeast Asia Freedom of Expression Network) indicates gaps in the protection of citizens' personal data, as well as the absence of independent oversight mechanisms. (Nath St Xavier et al., 2015) This highlights that, in addition to legal frameworks, the state must also cultivate a culture of respect for digital rights and equip citizens with critical awareness regarding the use of their data. Islamic International Law (IIL) is a discipline that seeks to bridge the principles of Sharia with international legal norms, including Human Rights (HR). In ISL, the concept of HR does not conflict with Islamic values, but rather can be strengthened through the *maqashid al-sharia* approach the primary objectives of Islamic law, which emphasizes the protection of five things: religion (*din*), life (*nafs*), intellect (*aql*), lineage (*nasl*), and property (*mal*). (Masorong, 2025) The protection of life (*ḥifẓ al-nafs*), for example, affirms the importance of individual life and safety, in line with international principles on the right to life and the right to personal security. In the modern context, the protection of life can be interpreted as efforts to guarantee the right to privacy, freedom from digital violence, and the security of personal data in the big data ecosystem.

Islamic human rights also place justice (*‘adālah*) as a core value in social life and the

legal system. Justice in the Islamic perspective is holistic, not only concerning the distribution of wealth or the enforcement of law, but also concerning the distribution of information and equal access to technology. In the context of digital human rights, Islamic principles of justice can be used to assess whether algorithmic systems and the distribution of digital data create new inequalities, such as discrimination against minorities or violations against vulnerable groups. (Muhammad, n.d.) Islamic justice also demands accountability for the abuse of digital power, whether by the state or technology corporations. This is in line with the concept of accountability in contemporary human rights. Amid the challenges of globalization and digitalization, contemporary thinkers such as Mohammad Hashim Kamali and Tariq Ramadan emphasize the importance of an *ijtihad* approach to legal reasoning to address new issues such as digital privacy, artificial intelligence, and state surveillance. They suggest that the Islamic legal approach should not only focus on classical texts but also on its more flexible and transformative *maqashid*. In this regard, Islamic law has the potential to serve as an alternative ethical framework capable of balancing technological progress with the protection of human dignity. This approach aligns with global trends promoting the integration of moral values into technological design.

2. METHODS

This study uses a qualitative-descriptive approach to examine the intersection between the use of big data and the protection of human rights from the perspective of Islamic International Relations. The research primarily involves conceptual and normative legal analysis, supported by a literature review of both Islamic jurisprudence (*fiqh* and *maqāṣid al-sharī'ah*) and international human rights law. Data was collected through systematic review of academic journals, official reports from international institutions (e.g., United Nations Human Rights Council, Amnesty International), Islamic legal sources, and relevant policy documents. Key references include recent discussions on digital rights, ethical AI governance, and Islamic ethics in global law. To ensure relevance and credibility, the study prioritizes peer-reviewed publications and high-impact journals published in the last five to ten years, such as EMBO Reports (Schneble et al., 2018), Journal of Big Data (Adadi, 2021), and International Journal of Law Reconstruction (Suwondo, 2023).

In addition to textual analysis, a case study approach is applied to contextualize the role of big data in human rights violations, with examples drawn from conflicts such as Israel–Palestine and digital surveillance regimes in authoritarian states. Each case is examined using the ethical lens of *maqāṣid al-sharī'ah*, particularly *ḥifẓ al-nafs* (protection of life) and *'adālah* (justice), as guiding principles. This approach allows for a multidimensional interpretation of big data ethics, incorporating not only legal obligations but also moral accountability. Although empirical fieldwork was not conducted, triangulation is ensured through cross-referencing multiple authoritative sources and frameworks. This enables a balanced assessment of how Islamic values can provide alternative pathways in responding to contemporary digital challenges.

3. RESULTS AND DISCUSSIONS

The Role of Big Data in Documenting Human Rights Violations

The emergence of big data enables real-time collection and analysis of large volumes of information, offering a powerful tool for documenting human rights violations, particularly in digital-based conflict zones. Technologies such as Google Earth, AI-driven drone analytics, and the Internet of Things allow monitoring of civilian areas with a level of accuracy and speed previously unattainable. For instance, during the Gaza conflicts, satellite imagery and drone-based data analytics enabled NGOs to track infrastructure damage and civilian casualties with high precision (Adadi, 2021). In the Israel–Palestine conflict, the use of InSAR and Sentinel-1 satellite systems provided evidence that over 60% of Gaza's infrastructure had been damaged. Organizations like Amnesty International and Forensic Architecture documented over 2,500 attacks, relying on metadata, timestamps, and AI tools to map incidents and verify their authenticity. These technological applications are essential in an era where conventional journalism faces access restrictions, and digital disinformation is prevalent (Putra et al., 2024).

The rationale for selecting this case study lies in its status as one of the most prolonged, media-covered, and technologically monitored conflicts globally. It provides a concrete context where digital tools have shifted the landscape of human rights advocacy. Moreover, the global political significance and the depth of digital repression present in this conflict allow for meaningful normative critique (Studi et al., 2018). Beyond the documentation, big data supports the dissemination of verified information that strengthens diplomatic pressure and legal advocacy. International legal frameworks, such as the UDHR and ICCPR, have begun integrating digital evidence satellite images, drone footage, and metadata into legal investigations (Dedi Anton Ritonga & Muhammad Ichsan, 2025). Article 17 of the ICCPR, for example, is increasingly cited in legal debates regarding surveillance and digital targeting.

Limitations and Ethical Challenges

Despite its benefits, big data presents critical ethical concerns. Key among these is the potential for manipulation, algorithmic bias, and surveillance misuse, especially when data governance structures are weak or unregulated (Zhang, 2018). For example, Israel's deployment of the Blue Wolf system demonstrates how biometric and facial recognition technologies can violate the right to privacy and freedom of movement, particularly when used against marginalized populations like Palestinians. Power asymmetry in global data access further exacerbates digital inequality. Superpowers often monopolize surveillance technologies and dictate data norms, leaving smaller nations with limited agency (Ridwan et al., n.d.; Suwondo, 2023). As seen in Russia's media monitoring during the Ukraine conflict, big data can be weaponized for disinformation and narrative control, raising critical questions about justice and equity in data regimes.

Big Data in Human Rights Enforcement Transformation: The Maqashid Syari'ah Perspective

Maqashid Syari'ah, the higher objectives of Islamic law, provide an ethical framework to evaluate the moral implications of big data usage. The core principles of *hifz al-nafs* (protection of life) and *'adalah* (justice) are especially relevant in digital contexts. These principles mandate not only the avoidance of harm but also the proactive preservation of dignity and fairness in information governance. Contemporary Islamic thinkers like Jasser Auda emphasize the dynamic nature of maqashid arguing that they must be responsive to evolving

social realities, including technological change. Thus, applying maqashid to digital ethics is a logical extension of Islamic legal philosophy, especially in addressing privacy, surveillance, and digital autonomy (Pertiwi & Herianingrum, 2024). Islamic International Relations (IR) further enriches this approach by offering a normative legal tradition that parallels the Universal Declaration of Human Rights. Rather than standing in opposition, maqashid principles can complement global norms, promoting digital justice rooted in both universal and theological values. In this context, the misuse of big data by powerful states not only violates international law but also the moral imperatives of Islam (Muhammadiyah Jakarta & Pendapatan Daerah Provinsi DKI Jakarta, 2023).

Relevance of Islamic Values in Humanitarian Technology

Modern Islamic thought places the principles of maqāṣid shari'ah, especially hifz al nafs (protection of the soul) and 'adl (justice) as the foundation for making technology a mandate, not a tool of oppression. (Pertiwi & Herianingrum, 2024) For example, Sheikh Abdullah bin Bayyah in his work Maqhosidul Mu'amalah invites cross-disciplinary dialogue to ensure that technological innovation does indeed bring benefits, not harm, in accordance with maqāṣid and inseparable from its social context. (Masorong, 2025) This thinking is relevant in today's Big Data, because technology must be developed and used by fulfilling the principles of transparency, accountability, and protection of human dignity. By incorporating these values, Muslims can become pioneers of ethics in global digital technology.

Islamic IR is a set of disciplinary norms that seek to bridge the principles of sharia that exist in the international realm, including in Human Rights (HAM). (Atqiya, n.d.) The concept that has been written and agreed upon in the UDHR does not conflict with the concept of Islam and the elements of maqashid sharia. Namely with an emphasis on protecting five things in it: religion (din), soul (nafs), reason (aql), descendants (nasl), and property (mal). In this case, the hifdzu nafs approach greatly influences how the use of Big Data affects human rights. (Muhammad, n.d.) In its implementation, hifdzu nafs plays a wider role beyond mere physical protection, so that this also applies to digital and broader social dimensions. As it should be, hifdzu nafs is in line with the principles of human rights which express the principle of freedom. Islam highly upholds the values of humanity and the rights that accompany it. The existence of Big Data as a technological development that makes it easier for humans, should be used to protect human rights, not to control and supervise, as a form of oppression that occurs.

Big Data in the eyes of Islam is not just a tool, but a digital mandate. Whoever controls the data, whether the state or a company, has a moral responsibility to maintain its confidentiality, not to misuse it, and not to damage human dignity. (Imam_iqbal,+Journal+manager,+11.+Artikel+Mahatva+Yoga+Adi+Pradana, n.d.) This concept is parallel to the concept of khilafah fil ardh in Islam, where every human being is a khilafah and leader in the world. Which is none other than, in its implementation, the technology created by humans (the power of technology) will still be held accountable in the afterlife. And in its use, the technology must help and benefit others. In line with the hadith that explains this:

خير الناس أنفعهم للناس

"The best people are those who are most beneficial to humans." (Narrated by Ahmad, ath-Thabrani, ad-Daruqutni. This hadith was authenticated by al-Albani in Shahihul Jami' no: 3289)

and the verse of the Qur'an that calls for doing good to others:

إِنْ أَحْسَنْتُمْ أَحْسَنْتُمْ لِنَفْسِكُمْ

"If you do good, you do good for yourselves." (QS. Al-Isra: 7)

Islam as a source of law also encourages the principle of 'adalah (justice) as the main value in public policy. Therefore, in digital diplomacy and human rights advocacy, Muslim countries should contribute to calling for and affirming their country's position in fighting disinformation, cyberwarfare, and digital profiling that targets civilians. The use of data must be weighed against justice, not just technical efficiency or commercial logic. (Zulfa et al., 2023) For example, countries with a Muslim majority can encourage data protection policies that are in line with the maqashid sharia: requiring transparency, strengthening user rights over their data, and condemning excessive digital surveillance. Islamic institutions can also play a role in fostering ethical-based digital literacy in the community, so that they are not easily trapped in destructive digital narratives.

From here, we can use the Israel-Palestine case as an initial step that we can form. Community support and the use of big data as a monitor of human rights violations, accompanied by the international community, and the Muslim community as a monitor of the implementation of Big Data transparency fairly and evenly. (Masorong, 2025) Digital platforms as a medium for preaching, big data as a supervisory body that bridges the path to global social justice, and maqashid sharia as a form of legal framework that leads to justice and the welfare of all people. With this paradigm, Muslims are not only consumers of technology, but also producers of inclusive and liberating global digital ethics.

4. CONCLUSION

The Big Data era has reshaped the landscape of human rights documentation and enforcement, particularly in complex conflict zones like Israel–Palestine and Russia–Ukraine. While this technology offers unprecedented transparency and efficiency in tracking violations, it also introduces serious ethical concerns, including surveillance overreach and digital inequity. This paper has shown that Islamic normative ethics through the lens of maqashid al-shari'ah, particularly hifz al-nafs (protection of life) and 'adalah (justice) can offer a powerful alternative framework to reorient digital technologies toward human dignity and social justice. Key contributions of this paper include: (1) integrating Islamic ethical thought with digital human rights debates; (2) presenting a concrete case study to illustrate digital power dynamics; and (3) proposing an inclusive vision for ethical digital governance that engages both civil society and Muslim-majority countries. The conclusion reinforces the central claim that Big Data should be treated not merely as a technical tool, but as a "digital mandate" a trust that demands accountability, equity, and a commitment to humanity. Ultimately, this ethical integration can inform a broader strategy for building just and compassionate digital futures through plural legal traditions and moral values.

REFERENCES

- Adadi, A. (2021). A survey on data-efficient algorithms in big data era. *Journal of Big Data*, 8(1). <https://doi.org/10.1186/s40537-021-00419-9>
- Atqiya, N. (n.d.). HAM DALAM PERSPEKTIF ISLAM.
- Baderin, M. A. . (2010). Hukum internasional hak asasi manusia & hukum Islam. Komisi Nasional Hak Asasi Manusia.
- Book, . (2021). Kebijakan dan Pelayanan Publik Berbasis Keadilan Sosial di Era Disrupsi dan Big Data. <https://www.researchgate.net/publication/357419756>
- Dedi Anton Ritonga, & Muhammad Ichsan. (2025). Hak Asasi Manusia (HAM) dalam Perspektif Islam dan Barat. *Politika Progresif : Jurnal Hukum, Politik Dan Humaniora*, 2(2), 193–204. <https://doi.org/10.62383/progres.v2i2.1771>
- imam_iqbal,+Journal+manager,+11.+Artikel+Mahatva+Yoga+Adi+Pradana. (n.d.).
- Masorong, A. N. P. (2025). ISLAMIC ETHICAL PRINCIPLES AND ACCOUNTABILITY IN GOVERNANCE. *Advanced International Journal of Banking, Accounting and Finance*, 7(21), 21–34. <https://doi.org/10.35631/aijbaf.721002>
- Muhammad. (n.d.). HAK ASASI MANUSIA (HAM) DALAM PERSPEKTIF MAQASHID AL-SYARI'AH.
- Muhammadiyah Jakarta, U., & Pendapatan Daerah Provinsi DKI Jakarta, B. (2023). INOVASI LAYANAN SISTEM INFORMASI PENELITIAN HUKUM DAN HAK ASASI MANUSIA (SIPKUMHAM) Dwiky Lucky Adiyasha (Issue 1).
- Nath St Xavier, A., Toshniwal, R., & Ghosh Dastidar Asoke Nath, K. (2015). Big Data Security Issues and Challenges. In *International Journal of Innovative Research in Advanced Engineering (IJIRAE)* (Vol. 2). www.ijirae.com
- Peminat, A. S., & Islam, K. (n.d.). PENGARUH KEKUASAAN ATAS PENGETAHUAN (Memahami Teori Relasi Kuasa Michel Foucault).
- Pertiwi, T. D., & Herianingrum, S. (2024). Menggali Konsep Maqashid Syariah: Perspektif Pemikiran Tokoh Islam. *Jurnal Ilmiah Ekonomi Islam*, 10(1), 807. <https://doi.org/10.29040/jiei.v10i1.12386>
- Putra, R. K., Fahmi Idris, M., & Widhiati, G. (2024). Perlindungan Data Pribadi Dalam Era Big Data : Implikasi Hukum Di Indonesia. 2, 31–44. <https://journal.stekom.ac.id/index.php/Jaksa>
- Ridwan, M., Arif Zulfikar, A., Kurniawati Br Pinem, R., Septiani, R., Sumantri Riyanto, O., & Pika Lbn Batu, D. (n.d.). HAM DALAM TINJAUAN BERBAGAI PERSPEKTIF HUKUM.

- Schneble, C. O., Elger, B. S., & Shaw, D. (2018). The Cambridge Analytica affair and Internet-mediated research. *EMBO Reports*, 19(8).
<https://doi.org/10.15252/embr.201846579>
- Serangan Israel berlanjut di Gaza, sasar warga sipil dan infrastruktur - ANTARA News. (n.d.). Sofian, M. (n.d.). PENEGAKAN HUKUM HAM DITINJAU DARI PERSPEKTIF HUKUM MAQASHID SYARIAH.
<https://nasional.kompas.com/read/2019/12/24/20042321/kaleidoskop-2019-catatan-komnas-ham->
- Studi, P., Bisnis, A., & Surabaya, U. (2018). PEMANFAATAN BIG DATA DAN PERLINDUNGAN PRIVASI KONSUMEN DI ERA EKONOMI DIGITAL Agung Pujianto 1) , Awin Mulyati 2) , Rachmawati Novaria 3). *Majalah Ilmiah BIJAK*, 127(2), 127–137.
- Suwondo, D. (2023). The Legal Protection of Personal Data in Islamic Perspective. *International Journal of Law Reconstruction*, 7(2), 221.
<https://doi.org/10.26532/ijlr.v7i2.33648>
- Universal Declaration of Human Rights Preamble. (n.d.). Zhang, D. (2018). Big Data Security and Privacy Protection.
- Zulfa, N., Millah, N. N., Nuratin, N., & Novitasari, K. (2023). KONSEP MAQASHID SYARIAH DALAM PRAKTIK STRATEGI PEMASARAN TIKTOK DENGAN LANDASAN ETIKA
- BISNIS ISLAM. AB-JOIEC: Al-Bahjah Journal of Islamic Economics, 1(2), 79–94.
<https://doi.org/10.61553/abjoiec.v1i2.64>