

THE COLLAPSE OF TRUST: Negotiating Amanah and Digital Sovereignty in Indonesia's Sacred Data Regime

Hassin Dzikry Ramadhan
Center for Religious and Cross-cultural Studies (CRCS), Universitas
Gadjah Mada, Indonesia
E-mail: hassindzikryramadhan@mail.ugm.ac.id

Abstract: The 2024 cyber crisis at Indonesia's National Data Center exposed more than a technical malfunction—it revealed a moral rupture in the state's handling of citizens' sensitive information. Public debate largely revolved around infrastructure and economic losses, leaving unaddressed the ethical fragility surrounding what this study terms sacred data: information about religious identities, practices, and communal networks consolidated by the state. Using Critical Discourse Analysis (CDA) and a relational ethics framework rooted in the Islamic notion of *amanah*, the article examines how technocratic governance has marginalized moral responsibility and silenced affected communities. Findings reveal that the incident gave rise to three interconnected risks: individual discrimination, erosion of communal autonomy through digital profiling, and geopolitical exposure, ultimately leading to data colonialism. These vulnerabilities point to a deeper failure of moral imagination—a crisis of *amanah* in the digital realm. The article argues that data must be reenvisioned as a sacred trust that links the state, society, and the divine. It concludes by calling for a transformation of Indonesia's data governance toward an *amanah*-based ethics that restores moral agency, ensures digital sovereignty, and redefines the social contract between citizens and the state in the age of technocratic power.

Keywords: *Amanah*, National Data Center, Relational Ethics, Sacred Data.

Corresponding Author: Hassin Dzikry Ramadhan

Article history: Received: January 25, 2025 | Revised: May 21, 2024 | Available online: June 01, 2025.

How to cite this article: Ramadhan, Hassin Dzikry. "The Collapse of Trust: Negotiating Amanah and Digital Sovereignty in Indonesia's Sacred Data Regime." *Journal of Islamic Philosophy and Contemporary Thought* 3, no. 1 (2025). <https://doi.org/10.15642/jipct.2025.3.1.68-88>.

Introduction

In mid-2024, Indonesia experienced a significant disruption to its national system due to a cyberattack on the National Data Center. This ransomware attack caused severe disruptions to various public

services,¹ including immigration operations and hundreds of other government administrative systems.² The incident immediately sparked widespread public discussion, although the conversation often focused on specific aspects.

The mass media, government, and cybersecurity experts have focused more on economic losses, evaluating the failure of national cybersecurity infrastructure, and debating attribution and institutional responsibility. The narrative that has emerged tends to focus on technical shortcomings and weaknesses in the country's digital defenses. However, behind this seemingly technical crisis lies a more fundamental issue that is often overlooked: the fundamental and critical vulnerability of personal data for millions of citizens, including Muslims.

The Data National Center project, as designed, is based on the principles of efficiency and modernization of state data management, with the primary objective of consolidating data from all ministries and state institutions into one large, centralized repository.³ The implication of this policy is the accumulation of highly personal and sensitive data belonging to citizens. One known dataset is managed by the Ministry of Religious Affairs, including religious affiliation data recorded by the Directorate General of Population and Civil Registration (Dukcapil).

This collection of data no longer serves merely as administrative records, but has become a digital representation of beliefs, spiritual practices, and communal bonds that are fundamental to society.

¹ Hendri Yaputra, "PDN Diretas, ELSAM: Pemerintah Gagal Lindungi Data Pribadi, Wajib Sampaikan Informasi yang Diretas," *Tempo*, June 24, 2024, <https://www.tempo.co/politik/pdn-diretas-elsam-pemerintah-gagal-lindungi-data-pribadi-wajib-sampaikan-informasi-yang-diretas--45867>.

² Cyprianus Anto, "PDN Diretas Berhari-hari, Bagaimana Nasib Data Pribadi Kita?" *Kompas*, June 28, 2024, <https://www.kompas.id/artikel/pdn-diretas-bagaimana-nasib-data-pribadi-kita>.

³ M. Riasetiawan, *Pusat Data untuk Pemerintahan* (Yogyakarta: FMIPA Universitas Gadjah Mada, 2016), 19; Tommy and M. I. P. Nasution, "Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah: Studi Pusat Data Nasional (PDN)," *Jurnal Manajemen Ekonomi Dan Bisnis (JMEB)* 4, no. 1 (2025), 2.

Within the Data National Center architecture, data on marriages issued by the Religious Affairs Office, data on hajj and umrah pilgrims, registration of endowment assets, lists of religious facility managers, and information on membership in religious-based community organizations are stored. As a result, the identity and social-religious networks of Indonesian society have undergone a process of digitalization and decentralization, which has then been consolidated into a single systemic architecture. This process, ultimately, reveals fundamental vulnerabilities within the system.

The lack of public discourse specifically addressing the risks to religious data reveals a rather alarming blind spot. When public attention is solely focused on material losses and general cybersecurity issues, the ethical and philosophical dimensions of this problem are overshadowed. The issue is not merely how data can be leaked, but extends to the fundamental question of what data is actually being collected and who has control over it.

The recent Data National Center case should serve as a moment for critical reflection on the consequences of state actions that, in the name of technocratic rationalization, reduce religion, which is something imbued with sacred meaning, history, and social relations, to nothing more than an administrative data variable that can be stored, regulated, and even exploited. This phenomenon highlights how a technocratic approach risks overlooking the profound aspects inherent in religion as a social and spiritual institution.

In this context, the application of critical analysis becomes very significant. Abeba Birhane, a philosopher of technology, highlights criticism of the “rationalism” paradigm that dominates the world of technology, where the complexity of human experience is reduced to mere data categories, allowing algorithms to work more efficiently.⁴ The government’s approach to implementing the Data National Center also appears to be a manifestation of such a paradigm.

Religion, which actually has complex theological and sociological dimensions, is reduced to data labels such as Islam,

⁴ A. Birhane, “Algorithmic Injustice: A Relational Ethics Approach,” *Patterns* 2, no. 2 (2021): 100205, <https://doi.org/10.1016/j.patter.2021.100205>.

Christianity, or Catholicism in databases for the sake of administrative convenience. According to Birhane, this way of thinking tends to overlook the principle of “relational ethics,” which holds that data is never truly neutral; data is always tied to the individuals and communities it represents, along with all the potential harms that entails.⁵ Thus, the issues surrounding the Data National Center can be seen as a result of failing to understand data as a relational entity, not merely an asset that can be collected or managed.

In Islamic intellectual tradition, knowledge (*ilm*) is not merely informational but relational, bound by trust (*amanah*) and responsibility. This conception resonates with relational ethics in the context of digital data, particularly when sacred or religious information is involved. From the relational ethical perspective on data proposed by Mhlambi and Tiribelli, a new dimension of analysis emerges related to the relationship between countries in the Global South and technological infrastructure. These thinkers highlight an important issue: dependence on technology and cloud services controlled by corporations and subject to foreign jurisdiction has the potential to create a form of contemporary data colonialism.⁶

Although the National Data Center was designed as a national project, in reality, its supporting infrastructure often still has ties to foreign companies, which are subject to foreign laws such as those of the United States. Moreover, information has recently surfaced that Indonesia has granted control over national data to the United States as part of a trade agreement.⁷ This poses a serious risk; religious data of Indonesian citizens, including that of Muslims, which can be categorized as strategic data related to demographics, affiliations, and social networks, could potentially be accessed by foreign government

⁵ Ibid., 8-9.

⁶ S. Mhlambi and S. Tiribelli, “Decolonizing AI Ethics: Relational Autonomy as a Means to Counter AI Harms,” *Topoi* 42 (2023), 867-868, <https://doi.org/10.1007/s11245-022-09874-2>.

⁷ Lia Hutasoit, “Transfer Data dalam Kesepakatan Dagang RI-AS Perlu Perhatian Serius,” *IDN Times*, June 24, 2025, <https://www.idntimes.com/news/world/transfer-data-dalam-kesepakatan-dagang-ri-as-perlu-perhatian-serius-00-sbfjr-g7pfsb?utm>.

entities for their geopolitical interests. This aspect highlights the importance of critical reflection on data sovereignty and the ethical challenges of the current digital age.

In this context, the state has indirectly reduced the “relational autonomy” that is the right of religious communities. In principle, religious organizations, whether mass organizations, churches, or mosques, have the inherent authority to protect the data of their members. However, when the state takes over this data and places it in a vulnerable system subject to foreign jurisdiction, this action not only demonstrates a failure to protect citizens’ rights but also has consequences for the decline of community sovereignty within it.⁸ The failure to protect religious data is no longer merely a matter of individual privacy but has evolved into an issue of communal security and a threat to national data sovereignty.

This research did not arise solely because of the Data National Center hacking incident, which on the surface appears to be purely technical. Upon closer inspection, this case actually reveals fundamental failures in the ethical and philosophical realm of data governance in the digital age. Religious data, which is inherently sacred and has communal value, is now treated like a commodity that is prone to leakage.

A technocratic approach that is insensitive to the local context ignores the unique risks inherent in this type of data. The state, in this case, seems to be neglecting its relational responsibility towards religious communities, which are an important foundation for the state, especially in a country like Indonesia. Seeing this gap in discourse, this paper aims to offer a deeper analysis of these risks, using a relational ethics perspective and a decolonial paradigm. It is time for issues like this to be studied in greater depth, not just superficially.

This paper employs a qualitative approach, focusing on an in-depth analysis of the discourse surrounding the National Data Center

⁸ Just Net Coalition, “Digital Justice Manifesto: A Call to Own Our Digital Future,” in *Data Ethics: Building Trust*, ed. C. Stückelberger and P. Duggal (Geneva: Globethics Publications, 2023), 319.

crisis and its impact on religious data in Indonesia. This paper not only pays attention to technical aspects on the surface but also seeks to uncover ideological assumptions, power relations, and ethical dimensions hidden behind the narrative. Therefore, the most appropriate method to use is Critical Discourse Analysis (CDA), as it can comprehensively and critically dissect the narrative to its root causes. CDA helps me critically examine the dominant discourse surrounding cybersecurity and economic losses. However, these discourses often overlook the specific vulnerabilities experienced by religious communities, so the vulnerability of these minority groups is frequently neglected in the main discussion.

Data analysis will follow the three-dimensional framework of CDA popularized by Fairclough, which integrates text analysis, discursive practices, and social practices. Text analysis: focuses on linguistic details in the data. The use of certain words and metaphors helps to understand how a particular framework of thinking is applied to the topic of this paper.⁹ The primary objective at this stage is to examine the role of language in shaping and influencing perceptions of various issues. Discursive practice raises key questions, including who is given the authority to speak as an expert, who is not represented or even marginalized, and how the media frames the incident. This analysis links the text to its social context of production, thereby enabling the identification of power relations, exclusion, and representation processes that occur within the media sphere.¹⁰

Social practices: theoretical frameworks such as those by Birhane, Mhlambi, and Tiribelli on the critique of rationality in data and relational offerings are used extensively.¹¹ This analysis explores the extent to which existing discourse reproduces or challenges ideologies that tend to reduce fundamental values. Additionally, dependence on foreign infrastructure, both explicit and implicit in the discussion, is analyzed to reveal power dynamics in a decolonial context.

⁹ Norman Fairclough, *Discourse and Social Change* (Cambridge: Polity Press, 1992), 69.

¹⁰ *Ibid.*, 78.

Quantitative content analysis may be able to count the frequency of the word ‘cybersecurity’ versus ‘privacy rights’, but it fails to unpack why one discourse becomes dominant and the other marginalized. CDA, on the other hand, is explicitly designed to explore the relationship between language, power, and ideology. In the case of Data National Center, the goal is not only to map what is said, but to reveal how language is used by state actors (such as Kominfo and BSSN) to frame the crisis as a technical failure, thereby effectively covering up deeper ethical and relational failures.

The narratives that emerged in the public sphere after the hacking incident at the National Data Center revealed a dominant narrative that systematically described this crisis in technical and economic terms. These findings can be divided into three main parts. *First*, mapping the hegemonic discourse shaped by the state and the mass media. *Second*, identifying “sacred data” that is highly vulnerable and often appears as a counter-discourse that receives little attention. *Third*, an in-depth analysis of the three dimensions of risk faced by religious communities as a consequence of data governance failures.

Hegemony of Discourses: Technical Failure as the Main Crisis

Shortly after public services were paralyzed by a ransomware attack on the Data National Center, the narrative constructed by government officials and then disseminated by the national media consistently focused on three main points: cybersecurity issues, potential economic losses, and national stability. The public discourse that developed continued to refer to these three pillars. Upon examining ministry press releases and major media coverage, the dominance of technocratic terminology becomes evident, such as: “cyberattack,” “digital defense fortress,” and “system recovery.” Such word choices are not merely stylistic but frame the issue as an external threat requiring technical responses and strengthened defenses.

In practice, the state deliberately placed officials from National Cyber and Crypto Agency (BSSN), Ministry of Communication and Informatics (Kominfo), and cybersecurity experts as the main actors in

the public narrative.¹² Their voices dominate explanations regarding the technical details of the attack, the negotiation process with hackers, infrastructure recovery measures, and even mutual blame. As a result, the public is led to view this crisis solely as a technical issue, as if it were solely the domain of engineers and security experts.

The president, quoted by Tempo, stated, "All of our national data is backed up, so that if something happens, we won't be caught off guard. This also happens in other countries, not just in Indonesia."¹³ Although this statement is technically valid, it tends to be normative, and discursively, it narrows the scope of the issue, often neglecting other dimensions. Another example, quoted from Kompas, is the statement by the Head of the Criminal Investigation Agency (Kabareskrim), Wahyu Widada: "In the process of enforcing the law, it is not something that happens suddenly; everything goes through a thorough process. Ransomware is not something easy to handle."¹⁴

Upon closer examination, the pattern of marginalization of certain voices is evident amid the crisis's dynamics. During critical periods, there is almost no space for discussion for representatives of religious organizations, the National Commission on Human Rights (Komnas HAM), or digital rights activists to raise issues regarding the impact of data breaches on vulnerable groups, except in some opposition media outlets like Tempo, which highlights the voice of ELSAM (Institute for Community Studies and Advocacy). Technocrats

¹² Prima Cyber Solusi, "Kronologi Diretasnya PDN Indonesia oleh Ransomware Brain Cipher," *Prima Cyber Solusi*, July 5, 2024, <https://www.primacs.co.id/post/kronologis-diretasnya-pdn-indonesia-oleh-ransomware-brain-cipher>; Siti Yona Hukmana, "PDN Diretas, Kominfo Disebut tak Minta *Back up* Data ke Telkom Sigma," *Media Indonesia*, July 29, 2024, <https://mediaindonesia.com/politik-dan-hukum/681490/pdn-diretas-kominfo-disebut-tak-minta-back-up-data-ke-telkom-sigma>.

¹³ Yaputra, "PDN Diretas, ELSAM."

¹⁴ Rachel Narda Chaterine and Krisiandi, "PDN Diretas, Kabareskrim: 'Ransomware' Bukan Hal Mudah Ditangani," *Kompas*, July 15, 2024, <https://nasional.kompas.com/read/2024/07/15/14414911/pdn-diretas-kabareskrim-ransomware-bukan-hal-mudah-ditangani>.

dominate public discourse, leaving community leaders and human rights defenders marginalized.¹⁵

This kind of framing effectively shifts citizens from being subjects with rights and privacy to passive objects that are merely “secured” by the state. This phenomenon is a clear manifestation of “rationalism” as criticized by Birhane, in which the complexity of human beings and their social relationships is ignored in favor of efficiency and technical control.¹⁶

Disappearing Discourse: Vulnerabilities of “Sacred Data”

Behind the various discourses mentioned above, one reality often escapes attention: the type of data collected extends far beyond mere administrative data. Studies of internal government policy documents and data structures within ministries and agencies reveal the existence of a category of data that I refer to as “sacred data.” This term builds on the World Council of Churches’ (WCC) February 2022 assertion that issues of digital justice are inherently theological. The WCC links digital challenges to issues that have long been the focus of the ecumenical movement, such as power, justice, equality, participation, and human dignity as a reflection of God’s image.¹⁷

This sacred data covers the most personal aspects of citizens’ religious identity and practices. If such data were to leak, the potential damage would not only be unique but also impossible to measure economically; the impact would be truly significant and go beyond mere material loss. Kammourieh et al. view privacy as part of human dignity, that is, the right of individuals to control their own personal information.¹⁸ However, Kammourieh et al. also emphasize that group privacy differs from individual privacy. This means that a group can

¹⁵ Yaputra, “PDN Diretas, ELSAM.”

¹⁶ Birhane, “Algorithmic Injustice.”

¹⁷ World Council of Churches, “A Vision of Digital Justice,” in *Data Ethics: Building Trust*, ed. C. Stückelberger and P. Duggal (Geneva: Globethics Publications, 2023), 328.

¹⁸ Kammourieh et al., “Group Privacy in the Age of Big Data,” in *Group Privacy: New Challenges of Data Technologies*, ed. L. Taylor, L. Floridi, and B. Van der Sloot (Cham: Springer International Publishing, 2017), 43.

still suffer losses even if the privacy of each individual member is protected.¹⁹ Thus, the issue of privacy is not limited to the individual level, but it also encompasses a collective dimension.

The religion column on ID cards managed by the Population and Civil Registration Office (Disdukcapil) can be considered the most basic form of religious affiliation data. However, there is actually much more specific data, such as data on hajj and umrah pilgrims registered with the Ministry of Religious Affairs. The information collected there is not limited to identity, but also includes financial and health information, as well as an individual's travel history. For communal relationship data, marriage records at the Religious Affairs Office (KUA) do not merely document the relationship between two individuals. Beyond that, this data also maps family networks and social relationships within the community. As such, this data is highly potential for tracing lineage or inter-family relationships.

The vulnerability of "sacred data" becomes clear when we dissect its components. Hajj pilgrim data contains not only names and addresses, but also sensitive health records (e.g., vaccination status, history of chronic diseases), financial information (paid or deferred status), and relational data (information on *mah}ram* or companions). Similarly, KUA marriage data not only records two individuals, but also maps family networks, guardian status, and even religious conversion history or previous marital status (polygamy). This is highly sensitive relational data whose mapping can be misused for communal profiling.

In the institutional and network realm, Data National Center systematically documents data related to the registration of religious community organizations, information on *zakāt* and *waqf* recipients and donors, as well as data on places of worship and their administrators, including taxation aspects.²⁰ Overall, this dataset forms

¹⁹ Ibid., 52.

²⁰ A. H. Al Baihaqy, M. A. S. A. Yuwana, A. P. A. Surya, and M. A. N. Fauzi, "Analisa Dampak Kebocoran Data Pusat Data Nasional (PDN) 2024 dalam Perspektif HAM," *Wicarana* 3, no. 1 (2025), 35. <https://doi.org/10.57123/wicarana.v3i1.167>.

a comprehensive mapping of the social, financial, and leadership infrastructure of religious communities in Indonesia.

In fact, this kind of data is almost always overlooked in public discourse after a hacking incident occurs. Statements issued by religious organizations such as the Ministry of Religious Affairs (Kemenag) or the Indonesian Council of Churches (PGI), if any, are generally normative and reactive, merely calling for “increased security” without providing a detailed explanation of the specific risks actually faced by their communities.²¹

This void indicates a failure in discursive practice. Even the most affected groups do not have adequate mediums or language to express their vulnerability, especially when the state’s technical narrative is so dominant. The state, in its role as data manager, appropriates communal information without establishing a proper public discourse on the relational responsibilities that should accompany it. Yet, group privacy is a crucial element of the global privacy perspective, especially in low- and middle-income countries (LMICs).²²

Analysis of the Consequences of Data Leaks on Religious Communities

Viewed through the lens of relational ethics, the leakage of this “sacred data” carries three closely interrelated dimensions of risk. At the individual level, the leakage of data related to religious affiliation can clearly open the door to discrimination. Sacred data, such as information about interfaith marriages or conversion histories, has a high potential for misuse, ranging from intimidation to social persecution. This discriminatory practice, through the lens of relational ethics, not only harms individuals materially, but also

²¹ Dodi Irawan Syarip, “Pentingnya Menjaga Keamanan Data EMIS 4.0 melalui Penerapan Sistem Manajemen Keamanan Informasi,” *Kementerian Agama*, September 21, 2024, <https://kemenag.go.id/opini/pentingnya-menjaga-keamanan-data-emis-4-0-melalui-penerapan-sistem-manajemen-keamanan-informasi-kGzPg>.

²² L. Taylor, “Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World,” in *Group Privacy: New Challenges of Data Technologies*, ed. L. Taylor, L. Floridi, and B. van der Sloot (Cham: Springer International Publishing, 2017), 13.

damage social relationships and trust, which are the foundation of an individual's existence in society. This aligns with Birhane's argument, emphasizing that ethics must prioritize the protection and improvement of material conditions for the most vulnerable and affected groups.²³

Furthermore, the collection and aggregation of data on membership of religious organizations, religious study groups, or church congregations creates opportunities for communal mapping and profiling. Both state and non-state actors can utilize this data to identify, monitor, and potentially control groups deemed "deviant" or "risky" politically. Such practices constitute a violation of the relational autonomy that every community should have in managing its membership and internal activities without disproportionate intervention or oversight. As a result, a chilling effect emerges, where individuals are reluctant to affiliate or engage in communal activities due to concerns about the potential misuse of their personal data.

In an increasingly complex socio-cultural context, Indonesia faces significant challenges due to its dependence on global technology infrastructure, which poses real geopolitical risks. As stated by Mhlambi and Tiribelli, the placement of citizens' data on platforms under foreign jurisdiction, as reflected in several Indonesian trade agreements, can be seen as a form of data colonialism in the digital age.²⁴

Such data as religious demographics, maps of places of worship, financial flows of religious organizations, and lists of religious leaders are strategic assets in the field of intelligence. For foreign countries, this data is extremely valuable for mapping Indonesia's socio-political conditions, identifying potential proxies, or even triggering sectarian conflicts for their geopolitical agendas. However, on the other hand, the public also faces economic losses. For example, in Surabaya, one

²³ Birhane, "Algorithmic Injustice," 2.

²⁴ Mhlambi and Tiribelli, "Decolonizing AI Ethics," 868.

umrah network was postponed.²⁵ The recent Data National Center crisis demonstrates that Indonesia's data sovereignty is not only threatened by anonymous cyberattacks but also by global power structures that treat citizens' data as a commodity in intergovernmental negotiations.²⁶

Thus, the state has not only failed to protect the privacy of its citizens but also risks jeopardizing the collective data sovereignty of its people. This failure is not merely a technical one, but a paradigm failure in adopting relational and decolonial ethics in its technological governance.²⁷ This phenomenon highlights the need to strengthen national data protection in the face of evolving global challenges.

The Politics of Data and the Crisis of Trust

The findings of this article, which highlight the dominance of discourse in the National Data Center crisis, clearly require further study to understand the root causes and impacts comprehensively. The Data National Center crisis cannot be viewed solely as a cybersecurity incident; rather, it represents a fundamental shift in power relations, knowledge production, and trust formation in the digital age.

1. Colonialism of Data

The narrative constructed by the state and the media, which systematically reduces this crisis to a technical and economic issue, is not neutral. This framing is an ideological maneuver that aligns with the argument presented by Couldry and Mejias as data colonialism. They argue that the current phase of capitalism is characterized by "the expropriation of human resources so that data can be continuously extracted from them for profit."²⁸ In the context of the Data National Center, the "resources" being expropriated are the social

²⁵ Irwanda, "Server PDN Diretas, Jaringan Umroh Surabaya Tunda Keberangkatan," *Berita Jatim*, June 28, 2024, <https://beritajatim.com/server-pdn-diretas-jaringan-umroh-surabaya-tunda-keberangkatan>.

²⁶ Nick Couldry and Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford: Stanford University Press, 2019), 7-8.

²⁷ Mhlambi and Tiribelli, "Decolonizing AI Ethics," 871.

²⁸ Couldry and Mejias, *Costs of Connection*, xiii.

and religious lives of millions of citizens, which are then abstracted into data.

The dependence of National Data Center infrastructure on global cloud service providers (such as Amazon Web Services, Microsoft Azure, or Google Cloud) creates real jurisdictional vulnerabilities. These companies are subject to the laws of their home countries, such as the US CLOUD Act, which allows the US government to request access to data stored by these companies, wherever that data is physically located, including in Indonesia. Trade agreements that address cross-border data flow further exacerbate this risk.

The government's approach to the Data National Center, which prioritizes efficiency and modernization, clearly reflects extractive logic. Religion, which has complex social dimensions and a sacred nature, is positioned as if it were merely "raw material" that can be exploited and processed. As Couldry and Mejias explain, this process transforms social relations into "data relations," where human interactions are mediated by digital devices and directed toward the extraction of data.²⁹

2. *Data Justice*

Data colonization accompanied by commodification processes shows how our public discourse still fails to truly highlight the risks to religious data. The current privacy framework, to be honest, is still very individualistic. However, referring to the findings in the Data National Center case, the most vulnerable data is actually communal data: membership data of mass organizations, congregational networks, and marriage records. This is where the concept of group privacy becomes highly relevant. As Taylor et al. point out, big data technology typically does not specifically target individuals, but rather groups categorized based on certain attributes or behaviors. They emphasize that "data analytics is directed at the group level... to formulate types, not tokens."³⁰

²⁹ Ibid.

³⁰ L. Taylor, "Safety in Numbers?" 2.

In Islamic intellectual thought, *‘ilm* (knowledge) is never neutral. It is entrusted (*amanah*) to humanity as both a gift and a responsibility. The Quran repeatedly reminds believers that knowledge entails accountability before God and creation. When we speak of “religious data,” therefore, we do not merely refer to digital information about faith practices or institutions. We speak of a sacred trust—an *amanah ma‘nawiyyah*—that links the divine, the human, and the technological. Violation, misuse, or careless exposure of such data thus becomes not only a technical breach but a moral rupture that undermines the spiritual sociology of trust that sustains communal life.

The religious data collected in the Data National Center is not just a collection of ordinary information; it forms the collective identity of a group.³¹ Information about who is married to whom, membership of congregations, and the locations of religious activity centers, when viewed collectively, plays a major role in defining the community. Violations of such data cannot be viewed merely as violations of individual privacy, but as threats to the integrity of the group itself.

Floridi asserts that in many cases, “it is the group, and only the group, not its members, that is correctly identified as the true holder of privacy rights.”³² When such data is leaked, the risks involved are not only experienced by individuals, but the entire community can become the target of stigmatization, discrimination, and even persecution. Thus, the protection of religious data must be viewed as the protection of collective rights, not merely individual rights.

Referring to Taylor's ideas, this issue is closely related to the broader framework of data justice. The Data National Center crisis can be analyzed through the three pillars of data justice that he has formulated. The first pillar is visibility. The state places religious communities in a position that is highly exposed to threats, both from

³¹ L. Floridi, “Group Privacy: A Defence and an Interpretation,” in *Group Privacy: New Challenges of Data Technologies*, ed. L. Taylor, L. Floridi, dan B. van der Sloot (Cham: Springer International Publishing, 2017), 94.

³² *Ibid.*, 85.

hackers and other state actors, without the consent or control of the communities themselves.

The second pillar is involvement. Religious communities are not involved in the decision-making process regarding how their sacred data will be consolidated, managed, and protected. The third pillar is anti-discrimination. Data leaks open up opportunities for systemic discrimination. The data can be used to carry out “social sorting,” so that certain groups may be labeled as risky or undesirable, whether for commercial, political, or security purposes.³³

For foreign actors, Indonesia’s “sacred data” is pure intelligence asset. This data not only maps demographics, but also social networks, financial flows (*zakat/waqf*), and leadership maps at the grassroots level. This data can be used to identify potential proxies, map groups considered “moderate” or “radical,” or even design disinformation operations to fuel sectarian conflict for their geopolitical interests.

3. *Loss of Trust*

Ultimately, this Data National Center crisis reveals how fragile trust between the public and public institutions is. As Onora O’Neill emphasizes, trust does not mean blind obedience, but rather the ability of individuals to assess whether an institution is trustworthy or not. Unfortunately, the government’s overly technical response, accompanied by a lack of accountability and transparency, has hindered the public from conducting such critical assessments. Rather than strengthening trust, this pattern has instead exacerbated the “culture of suspicion” as described by O’Neill.³⁴

The crisis of trust described by O’Neill operates on two levels. Domestically, the public has lost confidence in the technical and ethical capabilities of the state. Internationally, however, this crisis reveals a greater failure related to sovereignty. Dependence on foreign cloud infrastructure and data transfer agreements puts the country in a weak position. Not only has the state failed to gain the trust of its citizens, but it also appears to “over-trust” foreign jurisdictions,

³³ Taylor, “Safety in Numbers?” 4.

³⁴ Onora O’Neill, *A Question of Trust* (Cambridge: Cambridge University Press, 2002), 19.

ultimately leading to a state of “data colonialism.” The state has failed to act as the protector of its people’s sovereign data, both from the threat of hackers and from the threat of data extraction by other geopolitical powers.

The proposed solution, namely increasing accountability through a more sophisticated security system, essentially raises new issues. O’Neill critically highlights what he calls the “accountability revolution” in modern management, which focuses too much on performance indicators, audits, and managerial controls. He argues that such systems often “do more harm than good in terms of trust,”³⁵ as they emphasize procedural compliance rather than the actual quality of trustworthiness.

In the context of Data National Center, the promise of more advanced security systems in the future does not automatically address the ethical failures that have already occurred. Restoring public trust requires more than technological innovation; it necessitates acknowledgment of responsibility and a commitment to the values that have been violated.

This crisis clearly shows that the current social contract is outdated when it comes to dealing with the challenges of the digital age. People give their personal data to the government based on the assumption that it will be protected and handled responsibly. It is time to redefine the digital social contract, not merely by piling on technical regulations, but by strengthening the ethical foundations and data rights of citizens. As emphasized by the Just Net Coalition, the new digital social contract must be grounded in the fundamental principle that “data subjects must own their data, both individually and collectively.”³⁶ In other words, neither the state nor other parties can arbitrarily treat citizens’ data. This new framework must affirm data sovereignty as a fundamental right that cannot be ignored amid technological advancements.

Furthermore, the National Data Center crisis reveals more than institutional failure. It reveals a crisis of *thiqqah* (trust), which is

³⁵ Ibid., 57.

³⁶ Just Net Coalition, “Digital Justice Manifesto,” 319.

central to Islamic moral life. In Islamic ethics, *thiqqah* is not blind confidence but a covenantal relationship between the trustee and the trusted. It sustains social harmony because it is rooted in *amanah* and *'adl* (justice). When technological infrastructures fail to protect what is sacred, they fracture this covenant, producing alienation and suspicion. Restoring trust, therefore, requires more than cybersecurity reforms; it demands a recovery of *thiqqah* as a relational virtue, one that integrates transparency, humility, and mutual accountability before both society and the divine.

Concluding Remarks

The hacking crisis at the National Data Center actually represents a fundamental failure in Indonesia's data governance, not just a technical cybersecurity incident. This phenomenon shows how the state, with its highly technocratic and efficiency-oriented approach, has reduced the meaning of data, which should embody sacred values, collective beliefs, and social networks to mere administrative aspects. The focus on technical and economic narratives in responding to this incident obscures the deeper and more strategic dimensions of risk.

The National Data Center crisis exposes the erosion of trust in the digital ecosystem, reflecting a deeper disconnection between technology and the ethical principles of *amanah* that traditionally guide Muslim understandings of responsibility. As a result, violations of community privacy have become increasingly apparent, the potential for data colonialism has opened wide, and most crucially, the foundation of trust between the state and its citizens has become increasingly threatened. Therefore, the Data National Center incident must be interpreted as a moment of reflection that demands a comprehensive paradigm shift in data governance. Technical improvements are important, but they are not enough. Building a resilient national digital ecosystem requires a new approach: fair, relational, and sovereign data governance. This effort must begin with rebuilding a digital social contract that recognizes communal rights to

data, ensures community participation, and makes the dignity and trust of citizens the cornerstone of policy.

Bibliography

- Baihaqy, A. H. Al, M. A. S. A. Yuwana, A. P. A. Surya, and M. A. N. Fauzi. "Analisa Dampak Kebocoran Data Pusat Data Nasional (PDN) 2024 dalam Perspektif HAM." *Wicarana* 3, no. (2025): 31–37. <https://doi.org/10.57123/wicarana.v3i1.167>.
- Birhane, A. "Algorithmic Injustice: A Relational Ethics Approach." *Patterns* 2, no. 2 (2021). <https://doi.org/10.1016/j.patter.2021.100205>.
- Chaterine, Rachel Narda, and Krisiandi. "PDN Diretas, Kabareskrim: 'Ransomware' Bukan Hal Mudah Ditangani." *Kompas*, July 15, 2024. <https://nasional.kompas.com/read/2024/07/15/14414911/pdn-diretas-kabareskrim-ransomware-bukan-hal-mudah-ditangani>.
- Coalition, Just Net. 2023. "Digital Justice Manifesto: A Call to Own Our Digital Future." Dalam *Data Ethics: Building Trust*, disunting oleh C. Stükelberger and P. Duggal, 315–319. Geneva: Globethics Publications.
- Couldry, Nick, and Ulises A. Mejias. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press, 2019.
- Fairclough, Norman. *Discourse and Social Change*. Cambridge: Polity Press, 1992.
- Floridi, L. "Group Privacy: A Defence and an Interpretation." In *Group Privacy: New Challenges of Data Technologies*, edited by L. Taylor, L. Floridi, and B. van der Sloot. Cham: Springer International Publishing, 2017.
- Hukmana, Siti Yona. "PDN Diretas, Kominfo Disebut tak Minta Back up Data ke Telkom Sigma." *Media Indonesia*, July 29, 2024. <https://mediaindonesia.com/politik-dan-hukum/681490/pdn-diretas-kominfo-disebut-tak-minta-back-up-data-ke-telkom-sigma>.

- Hutasoit, Lia. "Transfer Data dalam Kesepakatan Dagang RI-AS Perlu Perhatian Serius." *IDN Times*, Juni 24, 2025. <https://www.idntimes.com/news/world/transfer-data-dalam-kesepakatan-dagang-ri-as-perlu-perhatian-serius-00-sbfjr-g7pfsb?utm>.
- Irwanda. "Server PDN Diredas, Jaringan Umroh Surabaya Tunda Keberangkatan." *Berita Jatim*, Juni 28, 2024. <https://beritajatim.com/server-pdn-diredas-jaringan-umroh-surabaya-tunda-keberangkatan>.
- Kammourieh, L., T. Baar, J. Berens, E. Letouzé, J. Manske, J. Palmer, D. Sangokoya, and P. Vinck. "Group Privacy in the Age of Big Data." In *Group Privacy: New Challenges of Data Technologies*, edited by L. Taylor, L. Floridi, and B. Van der Sloot. Cham: Springer International Publishing, 2017.
- Mhlambi, S., and S. Tiribelli. "Decolonizing AI Ethics: Relational Autonomy as a Means to Counter AI Harms." *Topoi* 42 (2023). <https://doi.org/10.1007/s11245-022-09874-2>.
- O'Neill, Onora. *A Question of Trust*. Cambridge: Cambridge University Press, 2002.
- Riasetiawan, M. *Pusat Data untuk Pemerintahan*. Yogyakarta: FMIPA UGM, 2016.
- Solusi, Prima Cyber. "Kronologis Diredasnya PDN Indonesia oleh Ransomware Brain Cipher." *Prima Cyber Solusi*, July 5, 2024. <https://www.primacs.co.id/post/kronologis-diredasnya-pdn-indonesia-oleh-ransomware-brain-cipher>.
- Syarip, Dodi Irawan. "Pentingnya Menjaga Keamanan Data EMIS 4.0 melalui Penerapan Sistem Manajemen Keamanan Informasi." *Kementrian Agama*, September 21, 2024. <https://kemenag.go.id/opini/pentingnya-menjaga-keamanan-data-emis-4-0-melalui-penerapan-sistem-manajemen-keamanan-informasi-kGzPg>.
- Taylor, L. "Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World." In *Group Privacy: New Challenges of Data Technologies*, edited by L. Taylor, L. Floridi, and B. van der Sloot. Cham: Springer International Publishing, 2017.

- Taylor, L., Luciano Floridi, and B. van der Sloot. "Introduction: A New Perspective on Privacy." In *Group Privacy: New Challenges of Data Technologies*, edited by L. Taylor, L. Floridi, and B. van der Sloot. Cham: Springer International Publishing, 2017.
- Tommy, S., and M. I. P. Nasution. "Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah: Studi Pusat Data Nasional (PDN)." *Jurnal Manajemen Ekonomi Dan Bisnis (JMEB)* 4, no. 1 (2025).
- World Council of Churches. "A Vision of Digital Justice." In *Data Ethics: Building Trust*, edited by C. Stückelberger and P. Duggal. Geneva: Globethics Publications, 2023.
- Yaputra, Hendri. 2024. "PDN Diretas, ELSAM: Pemerintah Gagal Lindungi Data Pribadi, Wajib Sampaikan Informasi yang Diretas." *Tempo*, June 24, 2024. <https://www.tempo.co/politik/pdn-diretas-elsam-pemerintah-gagal-lindungi-data-pribadi-wajib-sampaikan-informasi-yang-diretas--45867>.
- Yuliano, Cyprianus Anto. "PDN Diretas Berhari-hari, Bagaimana Nasib Data Pribadi Kita?" *Kompas*, June 28, 2024. <https://www.kompas.id/artikel/pdn-diretas-bagaimana-nasib-data-pribadi-kita>.