HJIRS HASANUDDIN JOURNAL OF INTERNATIONAL AFFAIRS

Volume 6, No 1, February 2026
ISSN: 2774-7328 (PRINT), 2775-3336 (Online)

# The Role of OECD in the Issuance of Indonesia's Personal Data Protection Law: A Norm Localization Approach

**Wulandari**
Department of International Relations, Universitas Indonesia
Depok, Indonesia 16424
wulan.lunar@gmail.com / wulandari32@ui.ac.id.

**ARTICLE INFO**
Received: 24 October 2025
Accepted: 18 February 2026
Published: 20 February 2026

**DOI**
10.31947/hjirs.v6i1.47921

**Abstract**

In Indonesia, data governance has traditionally followed a state-centric model, as portrayed in the Electronic Information and Transactions (EIT) Law in 2008. However, a notable shift occurred in 2022 with the enactment of the Personal Data Protection Law, signaling Indonesia's transition toward a more people-centric approach to data governance. The author argues that OECD, mainly those from EU, taken a big role in this changing perspective. This research aims to examine the influence of OECD as a multilateral organization by great powers in shaping perspectives on liberal data governance in Indonesia. Norm localization theory by Acharya suggests that success in this localization process depends on credible local actors and institutional compatibility. This study employed a process tracing research method to analyze official documents released by OECD, EU, and the Indonesian government up to 2022.The result of the research shows that Airlangga Hartarto and the Coordinating Ministry for Economic Affairs negotiate national legitimacy and local constraints while translating the OECD's liberal and open data governance agenda into tangible legal reform. Also, Indonesia's Presidency in G20 as well as data breach and cyber-incident during IMEI registration procedure since 2020 help accelerate the issuance of Personal Data Protection Law. By combining OECD normative influence with a domestic elite predisposed to liberalization, the adoption of the Personal Data Protection Law is more than mere policy transfer. It represents norm localization, where imported norms are reinterpreted, adapted, and entrenched into Indonesia's legal system.

**Keywords:** Personal Data Protection, Norm Localization, G20 Presidency, OECD, IMEI, Data Breach

## 1. INTRODUCTION

States worldwide are increasingly adopting digital technologies to enhance national security. These technologies are used across various government activities, including public service delivery, surveillance, national defense, and revenue collection. The widely recognized CIA Triad—Confidentiality, Integrity, and Availability—serves as a foundational framework in developing these digital technologies (Hossaina et al., 2025; Chundu et.al, 2025; Radoniewicz, 2025). Confidentiality refers to the responsibility of securing sensitive

data and preventing unauthorized access to ensure user privacy and data protection. Integrity requires service providers to maintain data authenticity, accuracy, and consistency throughout its lifecycle. Lastly, availability involves establishing mechanisms that allow authorized entities to swiftly and reliably access data and resources whenever needed. By incorporating the CIA Triad in the development of cyber governance, governments are expected to balance the dual objectives of securing national interests and upholding citizens' rights to personal data protection.

Data governance encompasses the technical, policy, and regulatory frameworks required to manage data throughout its value cycle, from creation to deletion, and across multiple policy domains such as health, research, public administration, and finance. Governments aiming to maximize the benefits of data are increasingly prioritizing data governance while addressing critical challenges including privacy, intellectual property, market competition, and citizen empowerment (OECD, n.d.). According to the OECD, Market Openness becomes one of seven key vectors driving data governance and digital transformation besides Access, Use, Innovation, Jobs, Society, Trust (OECD, 2020). Market Openness supports digitalization by fostering fair competition and reducing regulatory burdens. Digital technologies are also transforming international trade by lowering costs, enabling new value chains, and changing both the way and the types of goods and services traded especially with the rise of cross-border digital services and bundled offerings.

Nevertheless, national security must be realized through the creation of a sovereign cyberspace that simultaneously safeguards individuals' rights to data protection, particularly when such data are voluntarily provided for state use. Privacy must be regarded as a central pillar of data governance, particularly in alignment with the principle of respecting citizens' personal rights. Among Southeast Asian countries, Malaysia is often considered more progressive in this regard. The country enacted its Personal Data Protection Act as early as 2010, earlier than Singapore and the Philippines in 2012, and well ahead of Indonesia, which only adopted its data protection law in 2022. Malaysia has also established a dedicated regulatory body to oversee data protection of its citizens (Cheryl & Ng, 2022). These efforts reflect Malaysia's recognition of personal data as a form of private property that warrants the same level of protection as physical assets. It is imperative that national governments not only adopt technological solutions but also ensure that legal, ethical, and human rights considerations remain at the forefront of their cybersecurity strategies.

United Nations also recognizes the position of individuals in cyber realm. The Internet Governance Forum (IGF), the Open-Ended Working Group on Information and Communication Technologies (OEWG), and the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC) are three UN forums that mainly discuss security in cyberspace. These forums are central and continuing elements of UN cybersecurity governance despite their different thematic scopes, governance contributions and institutional developments (Herbst and Jacobi, 2024). Furthermore, more non state actors, civil society, academia, and non-government organization are involved in the cyber security governance to make sure that several civil concerns such as the consequences of hate speech, improper data security, social exclusion, human rights, and data privacy are included in cyber and data governance.

The concern over people as the center of security began after Mahbub Ul Haq (1992) wrote the 1992 Human Development Report at the end of the Cold War. He proposed the agenda of new humanity order. The spirit was reducing the gap between Global North and Global South, particularly in terms of economy, capital, human development, education, and technology. The Report also proposed new efforts to negotiate a North-South human compact, thereby supporting an ongoing process initiated by the UN Secretary-General. The 1992 Human Development Report was expected to give a contribution towards a new global dialogue which redefines global security as security for people, not only for land, that ensures

everyone in the world has equitable access to the entire range of national and global opportunities to develop his or her full human potential.

Mahbub's report marked the beginning of extensive research in international relations focusing on individuals or citizens as a primary concern of states. From a global governance perspective, the protection of citizen data is not merely a technical issue; it is a matter of public trust, state responsibility, and digital sovereignty. It raises questions of cybersecurity, privacy data rights, and digital human rights under international law. Therefore, it is essential for institutions that collect and manage personal data to implement multi-layered protection systems. They must also assure the public that the data they submit voluntarily is processed within a secure and accountable framework. This aligns with the principle of confidentiality in cyber governance, which emphasizes the ethical and legal obligation of both states and non-state actors to safeguard personal data.

In Indonesia, data governance has traditionally followed a state-centric model. Initiatives such as *Satu Data Indonesia* and the emphasis on standardization and integration of government data reflect a focus on enhancing administrative efficiency and achieving national data consolidation, often at the expense of individual citizen needs. Personal data protection has received limited attention in this framework, as exemplified by the Electronic Information and Transactions (EIT) Law, which approaches data governance from a state-oriented perspective. However, a notable shift occurred in 2022 with the enactment of the Personal Data Protection Law, signaling Indonesia's transition toward a more people-centric approach to data governance. It is as seen in the EIT Law, the state acts as the regulator and law enforcer in the digital space while in PDP Law, the focus is on the individual's rights over their personal data. It also indicates that EIT Law is to maintain public order, security, and law enforcement in digital environments, quite contrary to the people centric perspective in PDP Law, that mainly to protect the rights of personal data subjects. Here are the differences of these approach exemplified.

Table. 1. Differences between EIT Law and PDP Law

| Aspect | Electronic Information and Transactions Law (Law No. 11/2008, as amended by Law No. 19/2016) | PDP Law (Law No. 27/2022) |
|---|---|---|
| Empowered Actors | The state (via police, prosecutors, Ministry of CIT) as enforcers of criminal and administrative law | Individuals as data owners; the state acts as a facilitator and supervisor |
| Protection of Individuals | Limited-the use of personal data must be granted permission from the owner. | Strong-guarantees rights such as data access, correction, deletion, and objection |
| Data Subject Rights | Not explicitly regulated | Clearly defined (Articles 5-15), including right to information, correction, and erasure |
| Enforcement Instruments | Criminal sanctions and administrative fines for electronic violations (e.g., defamation, hoaxes) | Administrative fines, warnings, and other sanctions for violations of data subject rights |
| Role of State Institutions | Strong and dominant (police, Ministry of CIT, Prosecutors) | More balanced; includes plan for an independent data protection authority |

Source: Processed by Author, 2025

As seen in Table 1., Indonesian government tries to divert their focus from state to people security. It raises a question, why Indonesia changes its perspective from state centric to people centric approach in data protection governance? It is necessary to understand since the change will mark the beginning of data governance in Indonesia.

This paper examines issue on individual security in data governance, and how Indonesia has recently acknowledged it through Personal Data Protection law in 2022. The author argues that OECD has taken a big role in this changing perspective. This research aims to examine the influence of OECD as a group of great powers in shaping perspectives on data governance in Indonesia. The reason is that Indonesia is on the process of becoming OECD member, and issuance of PDP Law might be due to serving OECD's interest. It is in line with Indonesia's commitment to adopting a more people-centric approach that upholds human rights, as envisioned in the 1945 Constitution. By analyzing how external power dynamics affect national policymaking, the study seeks to highlight the importance of maintaining sovereignty in policy decisions, especially in areas as sensitive as data governance.

The significance of this research lies in providing insights into how the interests of global powers can alter the direction of a country's policies and the importance of prioritizing national interests and citizen welfare in response. It also serves to reaffirm Indonesia's commitment to personal data protection, especially considering that, as of 2025, the country has not issued any implementing regulations that provide technical guidance for the enforcement of the Personal Data Protection Law.

## 2. ANALITICAL FRAMEWORK

This study employs a qualitative research design with a primary focus to answer the reason behind the issuance of PDP Law in Indonesia using norm localization by Acharya (2009) as the framework. In his research, Acharya (2009) also put forward several reasons why a country engages in norm localization. First, the presence of a crisis, whether in security or the economy, impacts the state and drives the diffusion of norms. Second, the interests of great powers in responding to these crises influence other countries to adapt accordingly. This process is also mediated by other factors such as regime change, unique identities and values of local actors, and the effects of international demonstrations, all of which play a role in determining whether a country will localize or reject a norm.

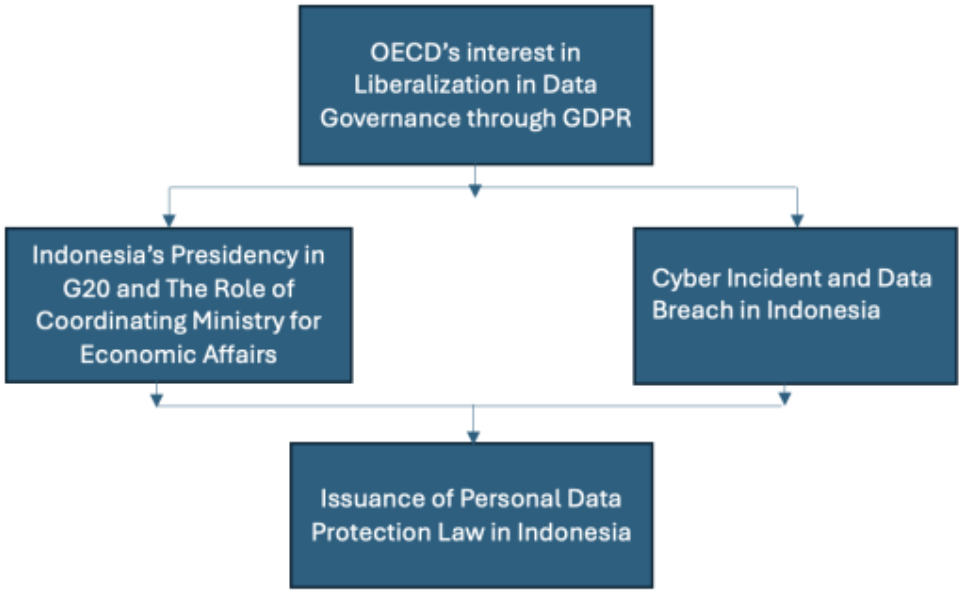
In the Localization phase, new tasks and mandates are created along with a set of policy instruments. Existing local norms are modified but not completely eliminated. Institutions that already exist continue to function but undergo reform or are assigned new core tasks. These reformed institutions become the driving force behind the diffusion of norms and the formation of new institutions. Localization reflects a complex process and outcome in which norm recipients construct a fit between transnational norms (including those previously institutionalized in a certain region) and local beliefs and practices. In this process, foreign norms that initially may not align with local norms are gradually integrated into the local normative framework. The success of norm diffusion strategies and processes depends largely on how much they allow for localization.

At this stage, reinterpretation and re-representation of external norms take place, including through processes such as framing (assigning new meaning) and grafting (attaching new elements). These processes may evolve into more complex forms such as reconstitution, which seeks to align foreign norms with pre-existing local normative orders (Acharya, 2004). The role of local actor acting proactively becomes more crucial in the process of norm localization. Additionally, institutional design, including both formal and informal rules and the organizational features of existing or emerging institutions, acts as both a constraint and a defining element of the social environment in which agents interact.

This study proposes that there are three reasons for adopting PDP Law in Indonesia. First, there is interest from western countries, mainly EU, in spreading liberalization in data governance for market penetration. Second, there is a local agent in Indonesia that believes in

the liberalization, and tries spreading it and adopt it to serve the big power interest. Indonesia's Presidency in G20 symbolizes a stronger commitment toward it. Lastly, there is a critical incident, namely cyber-attack and data breach that triggers the policymaker to launch PDP Law. In this case, the cyberattack in IMEI registration procedure become the case study of data breach. Therefore, the analytical framework for this paper is as follows.

**Diagram 1.** Analytical Model for Personal Data Protection Norm Localization in Indonesia's Data Governance




Source: Processed by the Author, 2025

## 3. RESEARCH METHOD

This study employs the qualitative process tracing method commonly used in political science studies. It can also be applied in the field of international relations, which examines the political dimensions of policymaking and the adoption of international norms. The processes within international organizations (IOs) in general, including negotiations and report drafting, provide important insights into the inner workings of multilateralism. Process tracing allows researchers to carefully follow and qualitatively examine complex multilateral processes as they unfold, documenting critical moments and evaluating the mechanisms that lead to specific outcomes (Rauch, 2023).

Process tracing is a form of analysis involving the systematic examination of diagnostic evidence, which is selected and analyzed based on the research questions and hypotheses formulated by the researcher. In this study, the data were gathered from released documents by OECD, EU, and the Indonesian Government before the issuance of PDP Law in 2022. Furthermore, the author also cited news, report, and review from reputable sources with the topics related to personal data protection, G20 forum and data breach in Indonesia. The author assumes that these topics will have implication to the issuance of Indonesia PDP law. The author used the gathered data to make analysis on the causal mechanism that led to liberal data norm localization in Indonesia.

Process tracing can make significant contributions to various research objectives, including identifying new political and social phenomena and describing them systematically. Also, it can evaluate existing explanatory hypotheses, discover new ones, and assess these new causal claims as well as gaining an understanding of causal mechanisms (Collier, 2011). The process tracing technique is chosen because it can explain the spread of liberalization on data

governance norm by OECD. Accordingly, this study can identify the historical background and international context underlying the development of the norm. This is important for the process of congruence building or identifying the alignment between the international and local contexts in Indonesia that facilitates the issuance of Personal Data Protection (PDP) Law in Indonesia.

## 4. RESULT AND DISCUSSION

In this section, the author elaborates three aspects that mainly push Indonesian government to adopt personal data protection norm into the national legislation. The first one is concerning the OECD's normative pressure for data liberalization in Indonesia. The author argues that data liberalization will lead to market liberalization that is strongly required by foreign investors mainly from G7 countries. Second, Indonesia's presidency in G20 becomes the crucial point, since in this forum, Indonesia through the Coordinating Ministry of Economic Affairs promises the foreign investors to create more transparent business environment through good governance and policy transformation. Lastly, several data breach in Indonesia and cyberattacks on official websites have also urged Indonesia to adopt PDP law.

### a. OECD's Interest and Pressure on Data Liberalization

The Organization for Economic Co-operation and Development (OECD) is an international organization that aims to shape policies that focus on individual welfare. Since its establishment, the Organization for Economic Co-operation and Development (OECD) has played a central role in global governance by providing strategic policy guidance to member and partner countries. The OECD helps governments shape policies that promote inclusive, resilient, and sustainable economic growth through its data-driven policy analysis and evidence-based recommendations. The organization serves as a platform for multilateral dialogue, consensus-building, and best practice exchange across key areas such as taxation, digital transformation, education, health, and environmental sustainability. The OECD has also become an influential actor in setting global norms and standards as part of its mission to foster better policies for better lives, particularly through its engagement with high-level global forums such as the G7 and G20.

In recent years, the OECD's work has extended into digital governance, recognising the transformative impact of data and technology on the global economy. In Going Digital Guide to Data Governance Policy Making, OECD has actively promoted frameworks around data openness, cross-border data flows, and trust-based digital economies, which have influenced the policy trajectories of many countries, including Indonesia (OECD, 2022). The organisation advocates for a balanced approach to digital governance that protects personal data while also enabling innovation and market openness. These efforts align with the OECD's broader commitment to building transparent, efficient, and interoperable digital systems that serve both economic and human development objectives.

The symbolic significance of the OECD being headquartered in France should not be overlooked. France has historically played a foundational role in shaping modern liberal political thought. The French Revolution of 1789 marked a turning point in the global discourse on democracy, human rights, and the rule of law that become principles underpinning many of the OECD's core values today. By situating its headquarters in a country that embodies revolutionary ideals of liberty, equality, and fraternity, the OECD's institutional identity is implicitly linked to a liberal internationalist vision of cooperation, openness, and shared prosperity. This legacy is also reflected in the OECD's emphasis on inclusive multilateralism, policy harmonization, and democratic accountability in global economic governance.

Therefore, the OECD's influence extends beyond technical policy advice. It plays a normative role in spreading liberal values through international cooperation and standard-setting. Its frameworks and policy guidelines often promote market liberalization, regulatory reform, and institutional transparency. These liberal principles resonate with the ideological foundations of many international agreements and national policies, particularly in emerging

economies like Indonesia that are actively engaging with global governance institutions. In the OECD's 60th Anniversary Vision Statement, OECD has mentioned their values, vision and priorities:

> *"We form a like-minded community, committed to the preservation of individual liberty, the values of democracy, the rule of law and the defence of human rights. We believe in open and transparent market economy principles. Guided by our Convention, we will pursue sustainable economic growth and employment, while protecting our planet."*[1]

The OECD's normative power thus not only facilitates economic integration but also helps shape domestic policy shifts in countries looking to align with international standards, especially in areas like data governance, digital economy regulation, and institutional reform. OECD countries have been in advance on personal data privacy and security. The Council of Europe and the European Union have been aware on securing citizens data and make regulation of cybercrime in EU countries (Radoniewicz, 2025). The Council of Europe's Convention on Cybercrime is the first international law act governing the subject, and the additional Protocol to the Convention on Cybercrime, dealing with the criminalization of computer-generated racist and xenophobic acts. European Union also has several regulations, including applicable European Union laws on cybercrime such as the Council Framework Decision 2005/222/JHA and Directive 2013/40/EU on attacks against information systems. Furthermore, the European Union has increasingly embraced digital sovereignty as both the ideological foundation and impetus for building its digital future in accordance with European values and principles, often driven by and intersecting with cybersecurity concerns as articulated in its 2020 Cybersecurity Strategy for the Digital Decade. However, the use of open-source software (OSS) in the region that may pose a threat to digital sovereignty (Tridgell, 2025).In navigating that issue, the EU has adopted closed language of digital sovereignty, with Cyber Resilience Act ('CRA') as key means for implementing the EU's strategy. These suggest that the Global North countries are mostly advanced when dealing sovereignty in the digital space.

Concerning data privacy protection, OECD refers to General Data Protection Regulation (GDPR) by EU. The GDPR promotes data privacy as part of human rights. In the GDPR, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), it is stated that:

> *The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.*[2]

This statement in the EU Directives explains that the processing of personal data must be designed to serve the interests of humanity. This is certainly the act of framing, as mentioned by Acharya (2009) in his theory. EU tries to link human rights and principle of freedoms to market openness. This is recognized in the Charter of Fundamental Rights of the European Union, as enshrined in the EU Treaties. It acknowledges the freedom of expression and access to information. Also, the Charter also mentions the freedom to conduct a business. That clearly explains the liberalization norm that EU member states uphold. With this value, EU and OECD countries demand open market access and economic liberalization values to spread, including in Indonesia.

This explanation underscores that personal data protection should not be understood solely as a technical or legal matter. Instead, it operates as a governance mechanism through which OECD countries promote open market access for developing states that rely on OECD

[1] OECD, 2021. OECD's 60th Anniversary Vision Statement
[2] EU, 1995. EU Directive 95/46/EC on 24 October 1995 concerning General Data Protection Regulation

funding. Indonesia, as a country that actively encourages foreign investment, has sought to demonstrate compliance with these standards by signaling its willingness to adopt the Personal Data Protection (PDP) Law. This development is consistent with Acharya's (2009) argument that the diffusion of international norms is often driven by the interests of Great Powers. In this context, the norm of personal data protection promoted by OECD and EU functions as a strategic instrument through which OECD countries exert pressure on other states to liberalize their markets and reduce trade barriers.

### b. Indonesia's Presidency in G20 and The Role of Coordinating Ministry for Economic Affairs in Adopting Liberalization in Data Governance

The Personal Data Protection Law (PDP Law) in Indonesia was designed with reference to the European Union's General Data Protection Regulation (GDPR). This paper argues that PDP Law is utilized to accommodate the interests of major powers, namely OECD countries that advocate for economic liberalization through more people-centric data governance. This approach promotes economic liberalization and increased private sector control, in contrast to a state-centric, centrally controlled economic model. The Personal Data Protection Law (PDP Law) was enacted alongside the launch of the 4th Indonesia-OECD Joint Working Group 2022-2025. Indonesia has expressed its intention to join the OECD since 2007, which has since been followed by Indonesia's accession roadmap to the OECD, targeted for 2024 (Ministry of Finance,2022).

According to the Norm Localization theory by Acharya (2009), the success of norm adoption depends on the local actor. The strong and legitimate local actors will determine whether an international norm can be accepted in a certain nation. In Indonesia's case, the research found that Airlangga Hartarto and The Coordinating Ministry of Economic Affairs fulfil this role. The PDP Law is included in the White Paper on Indonesia's National Digital Economy Strategy, which serves as one of the key supporting documents for Indonesia's accession efforts to become OECD members. In the White Paper on Indonesia's National Digital Economy Development Strategy 2030, there is an initiative to formulate implementing regulations for the PDP Law. These include detailed provisions on the roles and responsibilities of Data Protection Authority, as well as specific requirements for data protection impact assessments. In Q1 of 2024, a derivative regulation was issued to establish a Data Protection Authority. However, the full legal framework and implementing regulations have yet to be finalized as of mid-2025.

A central element of localization lies in the agency of local actors. Constructivist scholars contend that transnational moral entrepreneurs are tasked with mobilizing public opinion and political backing both domestically and internationally, facilitating the formation of like-minded organizations across borders, and advancing their objectives beyond narrow alignment with their own governments' national interests. Much of this effort is oriented toward influencing elite actors. The constitutive localization approach reframes norm entrepreneurship by shifting attention away from external actors advocating universal moral agendas toward domestic actors who promote a localized normative order that gains legitimacy through its alignment with broader universal norms.

Coordinating Ministry for Economic Affairs initiates the making of White Paper on Indonesia's National Digital Economy Strategy. It is plausible that Indonesia's Coordinating Ministry for Economic Affairs played a significant role in adopting OECD data governance norms, especially through an economic liberalization approach, under the leadership of Airlangga Hartarto. His education and career reflect liberal, market-oriented inclinations. Born in Surabaya in 1962, Airlangga earned his bachelor's in mechanical engineering from Gadjah Mada University in 1987, then pursued further postgraduate studies abroad: attending the Advanced Management Program at Wharton (University of Pennsylvania), obtaining an MBA from Monash University Australia, and a Master of Management Technology from the University of Melbourne. Before ascending to his current role as Coordinating Minister in 2019, he served as Minister of Industry (2016-2019) and held legislative positions related to trade,

industry, investment, and state-owned enterprises (Partai Golkar, n.d). His track record features involvement in broadly pro-market policies like industrial deregulation, incentives for private investment, and engagement in omnibus legislation reforms, all of which align with liberal economic values (Respatiadi & Tan, 2025).

The Coordinating Ministry for Economic Affairs, together with the Ministry of Finance, played a pivotal role as lead actors during Indonesia's G20 Presidency in 2022. This presidency marked a strategic moment for Indonesia to assert its influence on global economic governance, particularly in steering conversations on digital transformation and economic liberalization. The event presented new opportunities to deepen bilateral cooperation and promote the global diffusion of liberal norms. In his speech during G20's Presidency, Airlangga said:

> *Therefore, the G20 Indonesia Presidency carries the theme, Recover Together, Recover Stronger. With this theme, Indonesia's G20 Presidency is expected to provide a new spirit to create a world order that not only provides shared prosperity, but also ensures the sustainability of life in the future*.[3]

The combination of Airlangga's international business education, leadership in industry, and ongoing push for regulatory reforms lends credence to the view that he is inclined toward liberalisation in sectors including digitalization of data governance. This is depicted in the another Airlangga Hartarto's speech during the G20's Presidency:

> *At the same time, we will stand before the world's big countries to find a way out of the multiple disruptions that are hitting the world today, including health, economy, digitalization and environment sectors.* [4]

The concepts of *framing* in Acharya (2009) theory provide a more dynamic understanding of how emerging norms become aligned with pre-existing ones. Framing plays a crucial role in norm diffusion, as the connections between established norms and newly proposed norms are often unclear and must be deliberately constructed by norm advocates. Through framing, these actors draw attention to and actively shape issues by employing language that defines, interprets, and dramatizes them. Airlangga Hartarto's speech in G20 shows the act of framing. His statement is translated into the shift in data governance, aligning with Indonesia's ongoing digital agenda and data governance. Since 2016, the G20 has increasingly recognized digitalization as a key driver of economic growth and innovation. Under Indonesia's leadership, digitalization remained a central pillar of the G20 agenda, alongside global health architecture and energy transition. These priorities reflected Indonesia's intent to position itself as a forward-looking economy that embraces technological development not just for growth, but also for resilience and recovery, especially in the post-pandemic context.

One of the key milestones in the G20's approach to the digital economy was the elevation of the Digital Economy Task Force (DETF) to the Digital Economy Working Group (DEWG) during the Italy's presidency (Department for Digital Transformation of Italy, 2021). This institutional upgrade signified the growing importance of digital issues in global policymaking. Indonesia capitalized on this momentum by leading the DEWG in 2022, with the Ministry of Communication and Information Technology serving as the focal point. The country led high-level discussions focused on three priority issues: Connectivity and Post-COVID-19 Recovery, Digital Skills and Digital Literacy, and Cross-Border Data Flows including the principle of Data Free Flow with Trust (DFFT) (Coordinating Ministry for Economic Affairs, 2022).

On the G20 stage, Indonesia positioned itself as a normative actor in the digital governance landscape. The focus on cross-border data flows and trust-based frameworks is consistent with OECD and G20 efforts to promote data liberalization underpinned by robust

[3] Coordinating Ministry for Economic Affairs.2022. *Press Release* number HM.4.6/72/SET.M.EKON.3/2/2022 Jakarta, February 17th, 2022
[4] Coordinating Ministry for Economic Affairs.2022. *Press Release* number HM.4.6/166/SET.M.EKON.3/3/2022 in Jakarta, March 28th, 2022

safeguards. In this context, Indonesia's Personal Data Protection (PDP) Law can also be seen as part of a broader shift toward aligning domestic policies with international norms, namely balancing economic liberalization with the protection of citizens' digital rights.

### c. Cyber Incident dan Data Breach in Indonesia's IMEI Registration

Despite advancement in national digitalization, policies on digital technologies such as e-governance can create new vectors for cybercrime and undermine individual rights. For instance, the Netherlands identifies several common types of cybercrime, namely phishing, identity theft, hacking, website disruption or misuse, hate speech and terrorist incitement, and the distribution of illegal content such as pornography (Government of the Netherlands, n.d.). Among these, phishing, identity theft, and hacking are found in cyber governance as direct consequences of data breaches. Data breaches in the public sector pose severe threats to cybersecurity. These incidents not only violate existing security and privacy regulations but also erode public trust in government data management. Unlike breaches in the private sector, those involving state data can result in far-reaching consequences for both national and citizen security. As Hamid et al. (2025) note, the rise of sophisticated techniques. such as zero-day exploits, has made it increasingly difficult for law enforcement to track perpetrators' digital footprints. Existing regulations concerning data protection remain inadequate and require substantial improvement to effectively mitigate such risks.

The data breach in IMEI Registration Procedure highlights a critical friction at the heart of contemporary data governance: the conflict between state security objectives and the protection of personal data. This happens particularly to least developed and developing countries that tend to prioritize quantity over quality in digital development, focusing on popular initiatives, such as launching new applications or procuring digital tools, while neglecting the potential risks of data breaches (Chundu et.al, 2025).

Indonesia has implemented IMEI registration policy as part of its efforts to combat the influx of illegally imported used mobile phones for the sake of maintaining national security. Used goods are banned in Indonesia and viewed as posing various health, environmental, social, and economic risks. In terms of social and economic risks, items such as secondhand clothes, mobile phones, and laptops can undermine domestic industries, as they are sold at prices significantly lower than products from local enterprises and manufacturers. The country's low purchasing power and the desire of consumers to own branded goods at affordable prices have driven high demand for these used products.

**Table 2. Indonesia Phone Production Compared To Imported Phones**

| Year | Imported Mobile Phones (units) | Import value (USD) | Domestic production (units) | Number of Brands (Local & International) | Explanation |
|---|---|---|---|---|---|
| 2013 | 62 millions | USD 3 billions | 105.000 | 2 Local brands | High imports, very low domestic production |
| 2014 | 60 millions | Unknown | 5,7 millions | Unknown | Imports decreased slightly; domestic production grew significantly |

| | | | | | |
|---|---|---|---|---|---|
| 2015 | 37 millions | USD 2,3 billions | 50 billions | 23 local and international brands | Sharp decline in imports, huge rise in domestic production |
| 2016 | 18,5 millions | USD 775 millions | 68 billions | Unknown | Continued decline in imports; steady domestic growth |
| 2017 | 11,4 millions | Unknown | 60,5 millions | 11 local brands and 23 international brands. | Imports further declined, domestic production slightly decreased with more brands |

Source: *Indonesia Ministry of Information and Communication Technology*, 2019

The increasing demands for second mobile phone are worldwide, including in Indonesia. According to the International Data Corporation (IDC), global sales of used and refurbished phones surpassed 282 million units in 2022 (Kompas Tekno, 2023). The COVID-19 pandemic further fueled consumer interest in refurbished phones, which remain prohibited for import into Indonesia. Moreover, these imported secondhand phones often evade taxation, leading to two significant challenges for the state. First, the domestic industry loses competitiveness as these refurbished phones are sold at cheaper prices. Second, the government faces a loss of potential tax revenue from these untaxed imports.

In response, the Indonesian government mandated IMEI registration since 2020. This regulation is intended to curb the import of used devices. All imported mobile phones are required to have their IMEI numbers registered in the Central Equipment Identity Register (CEIR) system (Ministry of Communication and Information Technology, 2020). This regulation also applies to phones personally owned by individuals who previously lived abroad, whether Indonesian citizens or foreign nationals in order to use their devices legally in Indonesia.

The IMEI registration process mandates that citizens provide personal information, including their name, nationality, passport number, phone number, flight number, and details of the phone in front of Customs officer (Indonesian Customs, 2025). They are also required to pay duties and taxes since their phones are considered imported goods. However, this policy has unintentionally created new avenues for criminal exploitation, exposing vulnerabilities in an immature regulatory framework. Hackers also exploit weaknesses in the CEIR system by bypassing authentication and authorization protocols, enabling unauthorized IMEI registration that lead to data breach incident.

Indonesia launches IMEI registration policy originally intended to curb illegal mobile phone imports has inadvertently fostered the emergence of a black market for citizens' personal data. While the policy was designed to support state revenue and formalize the mobile device market, gaps in digital governance created vulnerabilities that have been exploited by criminal actors for personal gain. Several forms of misconduct have emerged in relation to this policy.

This study identifies a serious concern arises from the targeted cyberattacks on Indonesia's Centralized Equipment Identity Register (CEIR), the official system for IMEI registration (Tempo, 2023). These attacks occurred during the system's early implementation phase, exploiting its technical immaturity and the government's limited cyber defence capabilities. Moreover, it takes up to 2x24 for the IMEI data to be submitted to CEIR (Ministry of State Secretariat, 2020). This allows for higher vulnerability for data injection. All these factors illustrate the lack of preparedness and institutional resilience in managing critical digital infrastructure.

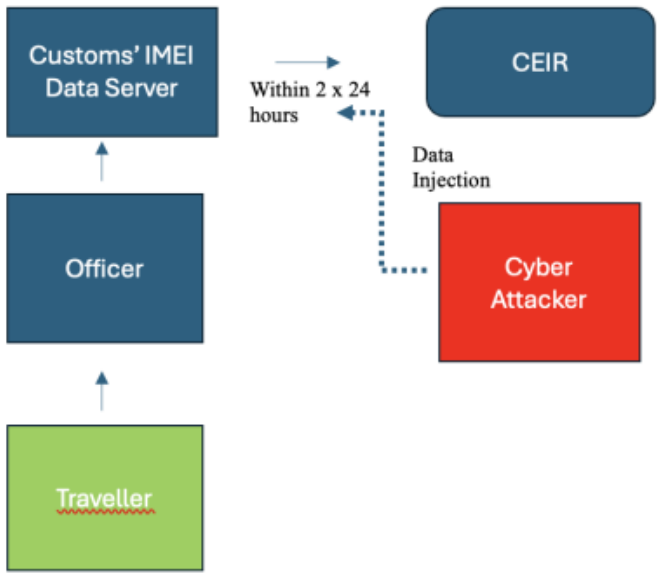
In order for mobile phones purchased or brought from abroad to be used legally in Indonesia, users must first register the device's IMEI number. There are four main methods by which individuals or entities can register imported mobile phones. The first method is by

personal use via postal shipment through Customs. Registration is typically conducted by the shipping forwarder, requiring the Consignment Note number and date or the Personal Import Declaration Document. Secondly, travelers can register their IMEI through Personal use via passenger baggage through Customs. The individual traveler registers the phone upon arrival by presenting their passport and boarding pass in front of the Officer, then providing personal data, including name, identification number, tax ID, flight/voyage/vehicle information, date of arrival, consignment details, and a valid email address or phone number. Thirdly, IMEI registration for commercial imports can be done through the Ministry of Industry. This process is conducted by authorized importers or distributors who are required to complete and submit all necessary import licenses and documentation before they can register the IMEI number of imported phones. Lastly, there is temporary activation via mobile operators using a tourist SIM card. This allows an imported device to have temporary IMEI activation for up to 90 days.

Among these four methods, the first, second, and fourth are particularly vulnerable to cyberattacks and personal data breaches. In the first two processes, facilitated through Customs and CEIR (Centralized Equipment Identity Register) systems, the IMEI registration procedure involves a dual-authentication system. During data transmission between these platforms, there is potential exposure to data injection or unauthorized access by cyber actors particularly during down time. This risk was especially pronounced during the early phase of CEIR implementation, when the system experienced overcapacity due to high volumes of incoming data. This situation created a technical bottleneck that may have been exploited by hackers or cybercriminals to inject illegally obtained IMEI data into the CEIR system.

These IMEIs are often sourced from smuggled phones, which may be new or refurbished and typically enter Indonesia through unmonitored border zones or unofficial ports of entry. Once these IMEIs are inserted into the system, the smuggled phones become operational—even though they have not passed through formal regulatory procedures.

**Diagram 2. Data breach scenario in the IMEI system**




Source: Processed by the Author, 2025

As shown in Diagram 1, the platform experienced significant system downtime during the early phase of the full implementation of Indonesia's Centralized Equipment Identity Register (CEIR) system for the IMEI registration procedure. This was largely due to the overwhelming volume of data submitted simultaneously, which exceeded the system's capacity. This

technical disruption created a critical vulnerability in the cybersecurity infrastructure of the state, enabling malicious actors to inject unauthorized IMEI data directly into the CEIR system, bypassing the legal registration procedures.

A key weakness in the implementation lies in the lack of real-time synchronization between the Customs system and the CEIR database. The delay between the time data submission through Customs and its final integration into CEIR introduces a critical window of exposure. During this interval, there is a heightened risk of data injection, manipulation, or cyberattacks, which can result in the unauthorized inclusion of IMEI data not processed through official channels.

Evidence of systemic abuse exists in the temporary IMEI registration procedure via tourist SIM cards. Criminal actors exploit this policy by selling tourist SIM cards to phone smugglers, enabling them to activate the IMEI of illegally imported phones for a 90-day period (Bisnis Tekno, 2022). Upon expiration, the IMEI can be reactivated by for the next 90-day period, effectively allowing repeated cycles of unauthorized use. All these vulnerabilities in data governance found in IMEI registration policy reveal broader challenges concerning data governance and digital infrastructure resilience. Moreover, the misuse of personal data in IMEI registration raises significant concerns regarding data privacy, digital rights, and trust in public institutions.

Besides data breach in IMEI registration procedure, there were multiple incidents of major data breaches involving BPJS Ketenagakerjaan (e.g. the alleged leak of 19 million BPJS Ketenagakerjaan records containing identity number, name, date of birth, email, etc.) that support the issuance of PDP Law (Kompas.id, 2023). In addition, there is also data breach case of BPJS Kesehatan, where data of 279 million citizens was suspected of leaking and was found to share identity structures with BPJS systems (Kompas.com, 2021).

The critical situation of data breach become one of the generic norms of new norm adoption, as mentioned by Acharya (2009). The security crises can generate demand for norm borrowing by calling into question 'the existing rule of the game'. These breaches not only raised public concern but also exposed legal and institutional gaps, prompting momentum for stronger regulation under the PDP law to protect digital rights and personal data despite growing cyber risks.

### d. The Issuance of PDP Law in Indonesia and the Shift toward Data Governance

The push for Indonesia's Personal Data Protection (PDP) Law can be seen as the product of both external normative pressure and internal dynamics. OECD advocacy for liberalised data governance and influences from global standards like the EU's GDPR have put pressure in developing economies like Indonesia to adopt the same standard for liberalized data governance. Moreover, internal dynamics, notably the leadership of the Coordinating Ministry for Economic Affairs under Airlangga Hartarto, who has often promoted economic liberalisation policies helps shifted Indonesia's perspective from a state-centric to a more people-centric norm in data governance.

Indonesia has established a legal framework for the protection of personal data through Law No. 27 of 2022 on Personal Data Protection (PDP Law), two year after the launching of IMEI registration policy. This legislation defines personal data as any information concerning an identified or identifiable individual, either independently or when combined with other information, whether processed through electronic or non-electronic systems. The law categorizes personal data into two types: General Personal Data and Specific Personal Data. General Personal Data includes publicly accessible information such as names, addresses, and phone numbers. Specific Personal Data refers to more sensitive categories of information that, if misused, could result in greater harm to the data subject, such as health records, financial data, and biometric identifiers. Indonesia also launches special websites dealing with personal data protection through www.pdp.go.id. Through the website, public can access information on the current issues, trends and regulation trajectories concerning PDP law.

The concepts of *framing* and *grafting* in Acharya (2009) theory provide a more dynamic understanding of how emerging norms become aligned with pre-existing ones. Framing plays a crucial role in norm diffusion, as the connections between established norms and newly proposed norms are often unclear and must be deliberately constructed by norm advocates. Through framing, these actors draw attention to and actively shape issues by employing language that defines, interprets, and dramatizes them. Grafting, by contrast, refers to a strategy through which norm entrepreneurs seek to institutionalize a new norm by linking it to an existing one, producing comparable prohibitions or obligations.

In formulating this legislation, the Indonesian government explicitly recognizes that the protection of personal data constitutes an extension of fundamental human rights, particularly the right to privacy as part of the broader right to personal security. This recognition is grounded in the 1945 Constitution of the Republic of Indonesia, elevating data protection to a constitutional and moral imperative. The PDP Law aims to safeguard citizens' rights to personal autonomy and privacy, promote societal awareness of data protection, and ensure respect for the dignity and identity of individuals in the digital sphere. In this stage, norm

Importantly, the PDP Law applies not only to individuals and public institutions within Indonesia but also to international organizations and foreign entities engaging in legal acts that involve data processing activities within the jurisdiction of Indonesia. This extraterritorial reach signals Indonesia's intention to align with global norms of data sovereignty and cross-border data regulation, asserting its regulatory authority over both public and private sectors (PDP, 2025a). The law is built on key legal principles including protection, legal certainty, public interest, utility, precaution, balance, accountability, and confidentiality. These principles reflect a commitment to embedding rule of law and rights-based governance in the digital domain. This reflects Indonesia's responsibility extends beyond national borders and into the transnational regulation of information flows.

To ensure effective enforcement, the PDP Law requires the issuance of Government Regulations. These are currently undergoing a harmonization process to align with existing legal and institutional frameworks (PDP, 2025b). This regulatory development is crucial for enabling institutional coherence and administrative capacity, both of which are essential to the realization of a functional and enforceable data protection regime. Through Law No. 27/2022, Indonesia is signalling its intent to be a responsible and active participant in the global governance of digital rights and cybersecurity. The law demonstrates a convergence between domestic constitutional principles and international norms and reflects the country's commitment to balancing state sovereignty with individual privacy rights, international cooperation, and regulatory accountability in the digital age.

The policy on IMEI registration in Indonesia was initially developed with the intent to uphold individual rights, particularly the right to property and digital security. According to the Director of Device Standardization at the Directorate General of Resources and Postal and Informatics Devices under the Ministry of Communication and Information Technology, the policy was designed not only to curb the circulation of illegal mobile phones but also to reduce the trafficking of stolen devices (Ministry of Communication and Information Technology, 2017). In practice, the system enables users to report stolen devices to law enforcement institution. Once reported, the phone's IMEI number can be detected and blacklisted within the national CEIR system, rendering the stolen device non-functional across all networks in Indonesia. In this way, the regulation is meant to protect citizens and deter digital property crimes, while ensuring that only legally registered and taxed devices can access domestic mobile infrastructure. The Director also refers to the same applicable regulations in foreign countries. Countries such as Turkey, Italy, Ukraine, Egypt, Kenya, Malaysia, Australia, New Zealand, and Pakistan have adopted policies for IMEI-based mobile phone regulation. Globally, the implementation of IMEI control systems has become increasingly common, particularly in countries where consumers are less inclined to purchase mobile phones bundled with postpaid services (Ministry of Communication and Information Technology, 2017). The Director further asserted that with the enforcement of this regulation, it should be impossible for illegally imported mobile phones

to operate in Indonesia. However, the reality on the ground reflects a more complex and dynamic situation. As is common in many regulatory contexts, criminal networks have demonstrated greater adaptability and technological sophistication than initially anticipated. By exploiting weaknesses in system integration, gaps in inter-agency coordination, and regulatory loopholes, various illicit schemes continue to circumvent the IMEI registration policy. These persistent violations highlight a broader issue within digital governance and transnational crime prevention.

To deal with issues on cybercrime and threat to data governance, United Nations on Drugs and Crime (UNODC) has proposed United Nations Convention against Cybercrime. The convention is issued with the goal of strengthening international cooperation for combating certain crimes committed by means of ICT systems and for handling serious crimes that demands the sharing of evidence in electronic form between member states (United Nations on Drugs and Crime, 2025). Adopted by the UN General Assembly on 24 December 2024 (Resolution 79/243), the United Nations Convention against Cybercrime is the first comprehensive global treaty addressing cybercrime through legal harmonization, technical measures, and international cooperation. Aiming to strengthen the global response to cyber threats, it promotes the sharing of electronic evidence, adapts traditional law enforcement tools to the digital environment, and embeds human rights safeguards. The Convention is open for signature on 25 October 2025 in Hanoi, Viet Nam, and remain open until 31 December 2026 at the UN Headquarters in New York. It will enter into force 90 days after 40 States ratify or accede to it. Once in force, a Conference of the States Parties will meet regularly to promote implementation and enhance state cooperation. As a landmark in global cyber governance, the Convention exemplifies multilateral norm-building and the growing role of international legal instruments in managing transnational digital threats.

Before the adoption of the United Nations Convention on Cybercrime, the Budapest Convention, established in 2001 by the Council of Europe, served as the first and most influential international treaty addressing internet and computer-related crimes through a harmonized legal framework. Although widely endorsed by many countries, Indonesia has not ratified the Budapest Convention, citing concerns over sovereignty, jurisdiction, and unequal negotiation processes that initially excluded many developing nations. However, Indonesia's recent bid to join the Organisation for Economic Co-operation and Development (OECD) marks a potential turning point. As the OECD promotes international standards on digital governance, cybersecurity, and cross-border cooperation, Indonesia's accession process may necessitate aligning with key normative frameworks supported by OECD members including the Budapest Convention. In this context, Indonesia's desire for deeper integration into global economic and digital governance regimes could increase the likelihood of future ratification, signalling a shift toward greater commitment to international cyber norms and legal harmonization.

## 5. CONCLUSION

Digitalization is evolving rapidly. It accelerates recovery through enhanced connectivity; on the other, Digital transformation is not merely about technology or lifestyle; it must serve to bridge divides, promote global balance, and support inclusive recovery. As data is increasingly a strategic commodity for information and decision-making, data governance must ensure security, utility, and ethical use. Control over data must be guided by strong principles that promote a better quality of life, not by motives to dominate the vulnerable.

By combining OECD normative influence with a domestic elite predisposed to liberalization, the adoption of the PDP Law was more than mere policy transfer; it represents norm localization, where imported norms were reinterpreted, adapted, and entrenched into Indonesia's legal and political system. Norm diffusion theory suggests that success in this process depends on credible local actors and institutional compatibility. In Indonesia's case, Airlangga Hartarto and the Coordinating Ministry fulfilled that role, negotiating national legitimacy and local constraints while translating the OECD's liberal data governance agenda into tangible legal reform.

Theoretically, this study supports the norm localization by Acharya (2009) that diffusion of international norms depends on the interest of great power, capability of local actors, and security crises, with the capability of local actors become the most crucial factor. This study also shows that both great power and local actors use framing to promote data liberalization norm. However, this study still faces limitation since other factors that might influence the norm adoption, namely domestic political change, uniqueness of actors, contagion effect, and international demonstration are not further elaborated. Future study can use these variables to analyze international norm adoption in Indonesia to strengthen the analysis.

Empirically, this study demonstrates that Indonesia's recent liberalization in data governance holds promises. By aligning with the data governance frameworks of the OECD and the European Union, Indonesia seeks to build trust among foreign investors, encouraging them to invest in its digital and economic sectors. This approach also supports Indonesia's aspiration to join the OECD, which emphasizes market openness, liberalized data flows, and seamless cross-border data transfer that become vital factors for international investors seeking reliable information about Indonesia's business climate. At the same time, people can also hope that Indonesia's government pay more attention to data privacy for individuals who have submitted their personal information for state use so that data breach incidents can be avoided or better mitigated in the future.

The challenge that Indonesia still encounters is as of 2025, Indonesia has yet to issue implementing regulations for the PDP Law. This delay raises questions about the country's actual commitment to data liberalization. This might also be a sign of institutional inertia or might reflect a deeper, more intrinsic stance in Indonesia's data governance approach: that state security takes precedence over individual data rights.

## 6. ACKNOWLEDGEMENT

The author sincerely thanks Ali Abdullah Wibisono, Ph.D. for his valuable insights and advice in writing this paper. The author also wishes to express deep gratitude to Prof. Evi Fitriani, Ph.D., as an academic advisor for her guidance and lessons on the norm localization approach, which greatly helped in understanding how international norms are adopted and localized into national policy. Lastly, the author extends sincere appreciation to the Indonesia Endowment Fund for Education (LPDP) for its financial support and commitment to advancing education for state apparatus.

## REFERENCES

Acharya, A. (2004). How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism. *International Organization, Vol. 58, No. 2 (Spring, 2004), pp. 239-275.* Stable URL: http://www.jstor.org/stable/3877858.

Acharya, A. (2009). *Whose Ideas Matter?: Agency and Power in Asian Regionalism*. Ithaca, NY: Cornell University Press, 2009.

Bisnis Tekno (2022). Memberantas Tipu-Tipu Jasa Unlock IMEI Palsu. Accessed on 21h July 2025 through https://teknologi.bisnis.com/read/20221212/280/1607666/memberantas-tipu-tipu-jasa-unlock-imei-palsu.

Cheryl, B.-K.; Ng, B.-K.(2022). Protecting the Unprotected Consumer Data in Internet of Things: Current Scenario of Data Governance in Malaysia. *Sustainability 2022, 14, 9893.* https://doi.org/10.3390/ su14169893.

Chundu, B., et.al. (2025). Cyber-security governance framework pillars for Zimbabwean local authorities, Cogent Social Sciences, 11:1, 2453094, DOI: 10.1080/23311886.2025.2453094.

Collier, D. (2011). Understanding Process Tracing. PS: Political Science and Politics, 44(4), 823–830. http://www.jstor.org/stable/41319974.

Coordinating Ministry for Economic Affairs of the Republic of Indonesia. (2022). Indonesia's G20 Presidency Focused on Strengthening the Multilateralism System and Effective Global Partnerships to Ensure "No One Left Behind". *Press Release* number HM.4.6/72/SET.M.EKON.3/2/2022 Jakarta, February 17th, 2022.

Coordinating Ministry for Economic Affairs of the Republic of Indonesia. (2022). Coordinating Minister Airlangga: Indonesia, together with the world's big countries, are looking for a way out of the multiple disruptions that plague the world. *Press Release* number HM.4.6/166/SET.M.EKON.3/3/2022 in Jakarta, March 28th, 2022.

Coordinating Ministry for Economic Affairs of the Republic of Indonesia. (2023).Launch of the White Paper on Indonesia's National Digital Economy Development Strategy 2030, Government Prepares 3 Phases of National Digital Transformation. *Press Release* in Jakarta, December 6, 2023.

Coordinating Ministry for Economic Affairs. (2023). *White Paper on the National Strategy for the Development of Indonesia's Digital Economy 2030*.

Department for Digital Transformation of Italy. (2021). Italian G20 Presidency: First Digital Economy Task Force Meeting at 10 February 2021. Accessed through https://innovazione.gov.it/notizie/articoli/en/italian-g20-presidency-first-digital-economy-task-force-meeting/ at 15th October 2025.

European Union. 2000. Charter of Fundamental Rights of the European Union (2000/C 364/01).

Government of the Netherlands,n.d. Forms of Cybercrime. Access on 21th July through https://www.government.nl/topics/cybercrime/forms-of-cybercrime.

Hamid, Supardi et.al. (2025) Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023. *Social Sciences & Humanities Open 11 (2025) 101234*

Haq, Mahbub ul. (1992). Human development in a changing world. *Human Development Report Office Series Occasional Papers.* New York : UNDP.

Herbst, Lena and Jakobi, Anja P. (2024). Opening up or closing down? Non-state actors in UN cybersecurity governance. *Journal of Global Security Studies, 9(3), 2024, ogae026*. https://doi.org/10.1093/jogss/ogae026

Hossaina, et.al. (2025). *Cybersecurity in local governments: A systematic review and framework of key challenges*. Urban Governance 5

Indonesian Customs (2025). *Customs Declaration (BC 2.2).* Accessed on 21h July 2025 through https://ecd.beacukai.go.id/

Indonesian Customs. (2022). Be*a Cukai Edukasi Masyarakat Ketentuan IMEI Melalui Mal dan Talkshow*. Accessed on 21h July 2025 through https://www.beacukai.go.id/berita/bea-cukai-edukasi-masyarakat-ketentuan-imei-melalui-mal-dan-talkshow.html.

Kompas Tekno, (2023). *IDC: Smartphone Bekas dan Refurbished Makin Diminati*. Accessed on 14th July 2025 through https://tekno.kompas.com/read/2023/01/12/12300087/idc--smartphone-bekas-dan-refurbished-makin-diminati#google_vignette

Kompas.id (2023).*Polri Amankan Enam Tersangka Pendaftar Nomor IMEI Ilegal pada Kementerian Perindustrian.* Accessed on 17th July 2025 through https://www.kompas.id/artikel/bareskrim-polri-ungkap-pendaftaran-nomor-imei-ilegal-pada-kemenperin.

Ministry of Communication and Information Technology (2025a). *Perlindungan Data Pribadi Frequently Asked Questions.* Accessed on 21st July 2025 through https://pdp.id/faq

Ministry of Communication and Information Technology (2025b). *Rancangan Peraturan Pemerintah Tentang Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.* Accesed on 21st July 2025 through https://pdp.id/rpp-ppdp/1?name=Rancangan%20Peraturan%20Pemerintah%20Tentang%20Peraturan%20Pelaksanaan%20Undang-Undang%20Nomor%2027%20Tahun%202022%20%20Tentang%20Pelindungan%20Data%20Pribadi

Ministry of Communication and Information Technology. (2015). *Kemkominfo Tengah Siapkan Aturan Registrasi IMEI Ponsel.* Accessed on 14th July 2025 through https://www.komdigi.go.id/berita/berita-komdigi/detail/kemkominfo-tengah-siapkan-aturan-registrasi-imei-ponsel.

Ministry of Communication and Information Technology. (2018). *Lindungi Hak Pengguna Ponsel, Kominfo Sosialisasikan Rencana Pengendalian IMEI.* Accessed on 14th July 2025 through https://www.komdigi.go.id/berita/berita-komdigi/detail/lindungi-hak-pengguna-ponsel-kominfo-sosialisasikan-rencana-pengendalian-imei.

Ministry of Communication and Information Technology. (2019). *Lindungi Industri dan Konsumen, Pemerintah Kontrol IMEI Ponsel.* Accessed on 14th July 2025 through https://www.komdigi.go.id/berita/berita-komdigi/detail/lindungi-industri-dan-konsumen-pemerintah-kontrol-imei-ponsel.

Ministry of Communication and Information Technology. (2008). Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions

Ministry of Communication and Information Technology. (2022). Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection

Ministry of Finance of the Republic of Indonesia. (2022). OECD-Indonesia Joint Work Programme 2022-2025 - *Fostering A Resilient, Sustainable And Inclusive Recovery . 14 Juli 2022.*

Ministry of State Secretariat for the Republic of Indonesia. (2020). *Government Implements IMEI Control for Telecommunication Devices Based on CEIR, September 16, 2020.* Accessed through https://setkab.go.id/pemerintah-terapkan-pengendalian-imei-perangkat-telekomunikasi-berbasis-ceir/ at 15th October 2025.

OECD. (2020). Going Digital Integrated Policy Framework. *OECD Digital Economy Papers*. February 2020 No. 292.

OECD. (2022). Going Digital Guide to Data Governance Policy Making.

OECD. (2022a). Meeting of the Council at Ministerial Level, 9-10 June 2022. The Secretary-General's Report to Ministers on the Implementation of the OECD Global Relations Strategy

OECD. (2024). *Roadmap For The OECD Accession Process of Indonesia* (Adopted By The Council By Written Procedure on 29 March 2024.

Partai Golkar, n.d. Airlangga Hartato's Profile. Accessed through https://www.partaigolkar.com/airlangga-hartarto/ at 15th October 2025.

Radoniewicz, Filip. (2025). *Cybercrime and the Law An Analysis of Legal Governance in Europe*.

Rauch, S. (2023). Process Tracing. In F. Badache, L. R. Kimber, & L. Maertens (Eds.), International Organizations and Research Methods: An Introduction (pp. 308-314). University of Michigan Press. http://www.jstor.org/stable/10.3998/mpub.11685289.63.

European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to The Processing of Personal Data and on the Free Movement of Such Data, And Repealing Directive 95/46/EC (General Data Protection Regulation)

Tempo. (2023). Membidik Tersangka Baru Kasus IMEI Ilegal. Accessed on 14th July 2025 through https://www.tempo.co/politik/membidik-tersangka-baru-imei-ilegal-822280.

Tempo, (2025). Bea Cukai Batam Tangkap Joki IMEI di Dua Pelabuhan, 42 iPhone Disita. Accessed on 21h July 2025 through https://www.tempo.co/digital/bea-cukai-batam-tangkap-joki-imei-di-dua-pelabuhan-42-iphone-disita-1203674#goog_rewarded.

Tridgell, Jennifer. (2025).Open or closing doors? The influence of 'digital sovereignty' in the EU's Cybersecurity Strategy on cybersecurity of open-source software. *Computer Law & Security Review 56 (2025) 106078*

United Nations on Drugs and Crime. (2025). *United Nations Convention against Cybercrime*. Accesed on 22th July 2025 through

https://www.unodc.org/unodc/en/cybercrime/convention/home.html#:~:text=Strengthening%20International%20Cooperation%20for%20Combating,the%20six%20official%20languages%20below.