ACTIO

INDONESIAN E-MAGAZINE FOR LEGAL KNOWLEDGE BY ANGGRAENI & Partners

EDITION #21 / MAY 2023

Digital Transformation of Procurement of Goods and Services in State-Owned Enterprises

Digital Sovereignty: Urgencies and Indonesia's Legal Frameworks

The Future of Education: Bridging the Gender Gap in Technology Skills

DIGITAL TRANSFORMATION TODAY: NAVIGATING THE CHANGING LANDSCAPE AND THE LEGAL IMPLICATIONS

9 772528 280004

ACT
AKASA CIPTA TAMA

We, Akasa Cipta Tama (ACT), was established in April 2015 as a response to the demand of highly qualified translators for business, legal, technical, and general documents; as well as interpreters and note takers for meetings, seminars, and conference. Our translators, interpreters and note takers have extensive experiences in their respective fields.

With a comprehensive database of qualified human resources, ACT works to ensure the best results in every project we run. Some of our top personnel have worked for various international events and some of our clients include the Office of the President of the Republic of Indonesia, People's Consultative Assembly, The United Nations, The World Bank, AusAID, USAID, and some prominent law firms in Indonesia.

Please do not hesitate to contact us if you have any question at marketing.akasa@gmail.com.
Looking forward to hearing from you.

CONTENTS

FOREWORD ---- 3

INFO: Digital Transformation of Procurement of Goods and Services in State-Owned Enterprises ---- 4

Q N A: Personal Data Controller and Processor According to Indonesia Personal Data Protection Law ---- 5

IN-DEPTH LOOK: Legal Implications of Artificial Intelligence-Powered Chatbots in Indonesia ---- 7

LAW LAB: Digital Sovereignty: Urgencies and Indonesia's Legal Frameworks ---- 10

ANALYSIS: Cloud-Based Processing and Data Protection Laws in Indonesia ---- 14

OPINION: Can Artificial Intelligence Finally Substitute The Legal Profession? ---- 18

LEADGAL: The Future of Education: Bridging the Gender Gap in Technology Skills ---- 20

TIPS: Tips on Communication Exchange to Mitigate Data Misuse ---- 25

ACTIO

Editorial:
Editor in Chief:
Setyawati Fitrianggraeni, PhD Candidate, FCIArb., FAIADR

Team of Managing Editors :
Dr. Hary Elias, BA V (Cantab), LL.M. (1st Class Hons), MBA (Columbia), Juris Doctor (HES)
Sri Purnama, S.H. (SPU)

Writers:
Tanya Widjaja Kusumah, S.H. (TWK)
Yoga Adi Nugraha, S.H. (YAN)
Eva Fatimah Fauziah, S.H., LLM. (EFF)
Reynalda Basya Ilyas, S.H., LLM. (RBI)
Fajrin Muflihun, S.H. (FJM)
Fildza Nabila Avianti, S.H., LLM. (FNA)
Fandy Mulyawan, S.H. (FMN)
Febriana Dwi Hapsari, S.H. (FDH)
Keshia Bucha, S.H. (KBA)
Deviana Bella Saputra, S.H. (DBS)
Ilma Aulia Nabila, S.H. (IAN)
Irvena Ayunya Dewanto, S.H. (IAD)
Jericho Xavier Ralf, S.H. (JXR)
Marcel Raharja, S.H. (MRA)
Sri Purnama, S.H. (SPU)
Jauza Marwa Salsabila, S.H. (JMS)

Media Consultant:
Fifi Juliana Jelita
Script Editor:
Wahyu Hardjanto
Visual Stylist:
Riesma Pawestri
Illustration: **freepik.com**

Actio Magazine is published every four months, made and distributed by:

ANGGRAENI and Partners

"The only way to make sense out of change is to plunge into it, move with it, and join the dance."

Alan Watts

Dear Readers,

Greetings and a warm welcome to the 21st edition of ACTIO!

As we progress further into 2023, we continue to witness the acceleration of digital transformation, driven not only by the global pandemic but also by the inexorable advancements in technology. In this rapidly evolving landscape, it is crucial to remain informed, adaptive, and collaborative.

With immense pride, ACTIO presents its latest edition: "Digital Transformation Today: Navigating the Changing Landscape and the Legal Implications." Our goal is to provide you with the knowledge and insights necessary to stay ahead in these transformative times.

In this edition, we delve into the heart of the digital revolution, exploring its effects on various aspects of our lives, both personal and professional. The articles in this issue aim to provide our readers with a deeper understanding of the legal implications surrounding the digital transformation, as well as insights on how to adapt and thrive in this ever-changing landscape.

Highlighting recent legal developments, our writers also examine the latest Indonesian laws and regulations related to digital transformation, including artificial intelligence, data protection laws, and the importance of cybersecurity in the digital era. Furthermore, we address the potential implications of these changes on both national and international levels, providing a comprehensive perspective on the subject matter.

We hope that this 21st edition of ACTIO offers valuable insights and serves as a useful resource for our readers as they navigate the complexities of the digital age.

Here's to embracing change, staying informed, and thriving together in the digital era!

Best Regards,

ANGGRAENI AND PARTNERS
Setyawati Fitrianggraeni, PhD Candidate, FCIArb., FAIADR.
Managing Partner

DIGITAL TRANSFORMATION OF PROCUREMENT OF GOODS AND SERVICES IN STATE-OWNED ENTERPRISES

Digital transformation of goods and services procurement through the e-catalog system is expected to reduce potential corruption in the government and State-Owned Enterprises (SOEs) because goods and services procurement activities will become more transparent.

Indonesian Ambassador to the United States (US) Rosan Perkasa Roeslani says that procurement transactions through e-catalog are faster than Electronic Procurement Services (LPSE). The Ambassador was of the view that the e-catalog is very effective in preventing corruption. Indonesia became the 13th partner of the United States Trade and Development Agency (USTDA) on June 3, 2021, especially in the Global Procurement Initiative: Understanding Best Value (GPI) initiative.

Based on existing partnerships, USTDA will train public procurement officials to achieve the greatest value for public infrastructure investment in Indonesia. The inclusion of Indonesia as a GPI partner was marked by the signing of a memorandum of understanding between USTDA and the Government Goods/Services Procurement and Policy Institute (LKPP) in 2021.

In addition, there are also concrete steps from the government by issuing Presidential Regulation (Perpres) number 17 of 2023 concerning the Acceleration of Digital Transformation in the Field of Government Procurement of Goods/ Services, promulgated on February 20, 2023. Through the presidential decree, the government assigned PT Telkom Indonesia Tbk to accelerate digital transformation in the field of government procurement of goods/services.
(MRA/TWK)

1. https://economy.okezone.com/read/2023/03/04/320/2775162/transformasi-digital-pengadaan-barang-dan-jasa-pangkas-potensi-korupsi-di-bumn?page=2
2. https://nasional.kontan.co.id/news/pemerintah-tugaskan-telkom-percepat-transformasi-digital-pengadaan-barang-dan-jasa.

PERSONAL DATA CONTROLLER AND PROCESSOR ACCORDING TO INDONESIA PERSONAL DATA PROTECTION LAW

What are the consequences for personal data controllers and processors who violate the provisions of Indonesia's Personal Data Protection Law?

Under the new Personal Data Protection Law Number 27 of 2022 ("UU PDP"), data processor and data controller (which means any individual that possess someone else's data) are subject to administrative sanctions. Article 57 covers the lack of seeking legitimate permission from data owners when collecting data, failure to convey information regarding the use and rights of a person's data, failure to provide a legally enforceable agreement between the data controller and data owner in using the data, and failure to comply with the usage purpose of the data.[1]

The administrative sanctions are:[2]

1) Written warning;
2) Temporary suspension of data processing activities;
3) Removal of the data handled by the processors; and/or
4) Administrative fine. (can be in the form of 2% (two percent) from annual income or annual receipt of variable violations)

However, the implementing regulations for UU PDP are still in drafting stage by Kominfo. Currently Kominfo is drafting the implementing regulation by involving experts in each sector of the industry to further strengthen the law.[3]

1. Chapter IV of UU PDP
2. Article 57 UU PDP
3. Kominfo, "Implementasi UU PDP, Kominfo Libatkan Asosiasi Secara Aktif", https://www.kominfo.go.id/content/detail/47433/siaran-pers-no-18hmkominfo022023-tentang-implementasikan-uu-pdp-kominfo-libatkan-asosiasi-secara-aktif/0/siaran_pers. Accessed on 3 April 2023.

What are the key differences between a personal data controller and a personal data processor, and what are their respective responsibilities under Indonesia's Personal Data Protection Law?

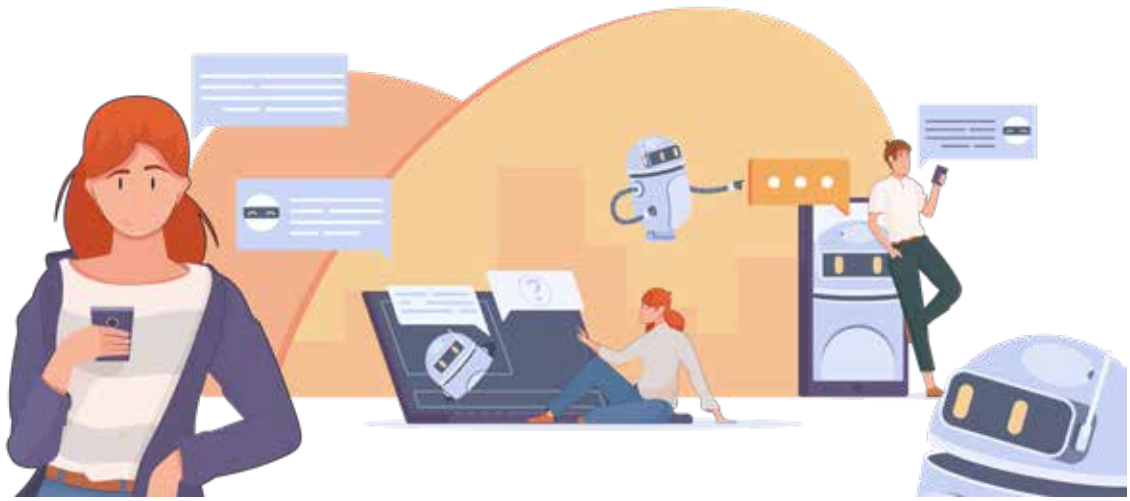
Data controller and data processors, include every person who holds someone else's data. Both have the responsibility to manage and take care of the data they possess. A data controller would have gained access explicitly from the data owners to conduct processing of the data. The law clearly states that data processors must convey information to data owners concerning the legality and data processing, the purpose of the data processing, types and the relevancy of the data processing, and any other details that are needed for the data owners to be aware of. In this regard, the data owner and data controller should enter into an agreement stating that the data controller has the right to the data in accordance with the activity that are agreed upon.[4]

In contrast with data controller, data processor's duty is to receive tasks from the data controller to process specified data. However, a data controller is also capable to process the data they may have in possession but the responsibility of what becomes of the data, will solely remain the data controller's responsibility.[5]

What are the requirements for obtaining consent from individuals before collecting, using, or disclosing their personal data under Indonesia's Personal Data Protection Law?

In an attempt to conduct processing of data, the data controller must first make an agreement with the data owner. According to the law, there must be a written agreement or recorded agreement between the controller and data owner to show the legitimacy of the consent given. The agreement must explicitly state that the data owner gives the right to the controller to conduct certain activities, depending on what the agreement to process was, and should be in a simple and easy-to-understand format. Further, the agreement must explicitly contain a clause regulating the data processing request, without which the agreement will be considered null and void.[6] Therefore, in any situation where the data controller is going to process a data owner's data, they must show an agreement for the data processor to proceed to the next step.[7] **(JRX/YAN)**

4. Article 20 UU PDP
5. Article 51 UU PDP
6. Article 22 UU PDP
7. Article 24 UU PDP



LEGAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE-POWERED CHATBOTS IN INDONESIA

With the robust development of technology in the current digital era, the utilization of Chatbots has become increasingly prominent. A chatbot is a computer program that can simulate human interaction by responding to simple queries or acting as digital assistants, offering increased personalization in the processing of information.[1] Through Artificial Intelligence ("AI"), automated rules, natural-language processing (NLP), and machine learning (ML), chatbots are able to process data and respond to various requests.[2] Chat Generative Pre-trained Transformer, commonly known as Chat GPT, is a type of chatbot that has increasingly gained popularity.[3] Among others, Chat GPT's notable ability includes providing natural and fluid response to its users and adapt to different situations, hence providing a more effective interaction.[4]

Despite the various benefits it provides, Chat GPT poses several risks towards cybersecurity. The ease with which Chat GPT can create code, write texts effectively, and impersonate others may easily be misused for ill intent, namely data theft.[5] Chat GPT can also be utilized to develop functional malwares, write phishing emails that appears convincing, spread misinformation, and write texts impersonating high-profile individuals, potentially leading to fraud.[6]

The human-like abilities of Chat GPT and the various risks it poses raise a number of questions namely: (i) Whether Chat GPT could be legally liable for its actions; (ii) The legally liable party, in the event that Chat GPT cause or contribute to harm to its users or third party; and (iii) The legal protection for Chat GPT users and the public. These questions will challenge law makers in every jurisdiction.

Currently, provisions related to the use of technology in Indonesia can be found in Law

1. OCI, "What is a Chatbot?," Oracle, April 17, 2023, https://www.oracle.com/id/chatbots/what-is-a-chatbot/.
2. *Ibid.*
3. Arimetrics, "What is ChatGPT," Arimetrics, April 17, 2023, https://www.arimetrics.com/en/digital-glossary/chatgpt#:~:text=ChatGPT%20is%20an%20intelligent%20chatbot,Chat%20Generative%20Pre%2Dtrained%20Transformer.
4. *Ibid.*
5. Malwarebytes, "What is ChatGPT?," Malwarebytes, April 17, 2023, https://www.malwarebytes.com/cybersecurity/basics/chatgpt-ai-security.
6. *Ibid.*

Number 11 of 2008 concerning Information and Electronic Transaction as amended by Law Number 19 of 2016 ("Law 11/2008"), Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions ("GR 71/2019"), and Law Number 27 of 2022 concerning Personal Data Protection ("Law 27/2022").

According to Art. 1 par. (8) Law 11/2008, "*Electronic Agent is defined as the device of an Electronic System made to perform an action on a particular Electronic Information automatically operated by a Person*".[7] Based on such provision, Chat GPT could be categorized as an Electronic Agent.

Furthermore, based on Art. 36 par. (2) GR 71/2019, Electronic Agent is considered as a part of an Electronic System, in the case where the Electronic System Operator operates with its own Electronic System or through an Electronic Agent. According to Art. 1 par. 6(a) Law 11/2008, "*Electronic System Operator is any Person, state operator, Business Entity, and communities that provide, manage, and/or operate Electronic Systems, either individually or jointly to the users of Electronic Systems for their own needs and/or the needs of other parties*". [8]

Based on the provisions above, it can be inferred that, in the implementation and the use of Chat GPT, the current regulations has classified an Electronic System Operator which may refer to the company that provides AI services of Chat GPT.

GR 71/2019 regulates both the responsibilities of Electronic System Operators and the operator of an Electronic Agent. According to Art. 14 par. (1) of GR 71/2019, Electronic System Operators are required to implement the principles of Personal Data protection in processing Personal Data, among others, (i) Collection of Personal Data to be carried out in a limited and specific manner, legally, fairly, with the knowledge and consent of the owner of the Personal Data; (ii) Processing of Personal Data to be carried out according to its purpose; and (iii) Processing of Personal Data to be carried out by protecting the security of Personal Data from loss, misuse, unauthorized access and disclosure, as well as alteration or destruction of Personal Data.[9]

Furthermore, according to Art. 40 par. (1) of GR 71/2019, the responsibilities of the operator of Electronic Agents, among others include: (i) Possessing and implementing policies and procedures to take action if there are indications of data theft;[10] (ii) Developing and implementing methods and procedures to protect and/or keep confidential the integrity of data, records, and information related to Electronic Transactions.[11]

In this vein, Article 2 in conjunction with Article 4 of the Ministry of Communication and Information Technology Regulation No. 5 of 2020 on Operation of Private Electronic System as amended by Ministry of Communication and Information Technology Regulation No. 10 of 2021 stipulate that foreign Private Electronic System Operators that provide services in Indonesian territory must be registered with the Ministry of Communication and Information and Technology. At the time of publication of this

7. Indonesia, *Law concerning Information and Electronic Transactions,* Law No. 11 of 2008 as amended by Law No. 19 of 2016 concerning Amendment to Law No. 11 of 2008 concerning Information and Electronic Transactions, SG No. 251 Year 2016, SSG No. 5952, Art. 1 par. (8).
8. Indonesia, Law 11/2008, Art. 1 par. 6(a).
9. Art. 14 par. (1).
10. *Ibid,* Art. 40 par. (1) letter (b).
11. *Ibid,* Art. 40 par. (1) letter (d).

article, Chat GPT/Open AI is still not registered in Indonesia.[12] Consequently, the obligations under the laws cannot yet be effectively enforced to the use of Chat GPT in Indonesia.

In addition, Law 27/2022 regulates the responsibilities of Personal Data Controllers and Personal Data Processors, and measures to protect individuals who possesses Personal Data.[13] According to Art. 1 par. (4) and (5) of Law 27/2022, "*A Personal Data Controller is any person, public body and international organization that acts individually or jointly in determining the purpose and exercising control over the processing of Personal Data"* [14] and *"A Personal Data Processor is any person, public body and international organization acting individually or jointly in processing Personal Data on behalf of the Personal Data Controller*".[15]

The "person" is defined as an individual or corporation. Based on the provisions above, both the operator and the user of Chat GPT can be categorized as processor and controller depending on whether in the use of AI, the operator and user determines the purpose of the processing when disclosing the personal data information to the system. Consequently, the obligations of a personal data controller and processor governed under Law 27/2022 which mirrors the European Union General Data Protection Regulation ("GDPR") shall apply in the use of Chat GPT.

In conclusion, Law 11/2008 and GR 71/2019 contain provisions pertaining to the responsibilities of Electronic System and Electronic Agent Operators, and enforcement mechanisms where such responsibilities are violated. Law 27/2022 further regulates the mitigation measures for failure to protect personal data. However, the legally liable parties involved in the use of Chat GPT as in other AI in practice, are not that straightforward. Other than the "operator" and "user", there are the developer, data provider, programmer, designer, manufacturer, owner of the data and the system itself. If the use of Chat GPT causes harm to a third party, there are many factors to be considered in determining liability such as what caused the damage, the action of the users, the level of control of the developers, and other aspects of the interactions between the different players.

To ensure utmost protection for Chat GPT users, the current regulations can be strengthened by: (i) Including an explicit definition of AI and a compliance framework; (ii) Including provisions that are tailored to the nature of AI and to address the misuse of AI and public protection; (iii) The issuance of relevant data protection regulations as mandated by Law 27/2022 promptly; and (iv) Ensuring the accountability and capacity of the Institution that will implement personal data protection, pursuant to Art. 58 par. (2) Law 27/2022. **(IAD/FDH/RBI)**

12. Kominfo, "Perusahaan Anda Termasuk Penyelenggara Sistem Elektronik?," Kominfo, April 24, 2023, https://pse.kominfo.go.id/home/pse-asing.
13. Indonesia, *Law concerning Personal Data Protection*, Law No. 27 of 2022, SG No. 196 Year 2022, SSG No. 6820, Art. 1 par. (6).
14. *Ibid*, Art. 1 par. (4).
15. *Ibid*, Art. 1 par. (5).
16. *Ibid*, Art. 1 par. (7).

DIGITAL SOVEREIGNTY: URGENCIES AND INDONESIA'S LEGAL FRAMEWORKS

INTRODUCTION

On the 15th March 2023, Indonesia's President, Joko Widodo raised worry about government workers using international credit cards.[1] He desires that the country's card issuer safeguard transactions from potential US penalties, as was done to Russia, whilst also reducing reliance on foreign companies and asserting greater control over the country's financial transaction. Last year, the government introduced the Government Credit Card (KKP) scheme for domestic use by government organisations and employees.[2] Whilst it has yet to be widely embraced, President Joko Widodo's drive is anticipated to increase local acceptability before they seek to internationalise it.

This statement raises the topic of Digital Sovereignty and why it is important for nations, in this context is Indonesia, to start considering of switching its dependency on international services to building its own. Floridi (2020) found that digital sovereignty is a central element in policy discourses on digital issues, but it remains highly contested. Meanwhile,[3] Pohle and Thiel through their work "Digital Sovereignty", suggested that digital sovereignty is understood more as a discursive practice in politics and policy than as a legal or organisational concept.[4]

According to Couture, the concept of digital sovereignty is used to describe various forms of independence, control, and autonomy over digital infrastructures, technologies, and data.[5] Whilst the notion of digital sovereignty is generally used to assert some form of collective control of digital content and/or infrastructures, the interpretation, subject, means and definition of sovereignty can significantly differ.[6] However, the urgencies to implement this are still needed to be scrutinised as well as Indonesia's capacity on creating digital independence from foreign parties' interferences. Is Indonesia ready? What should we expect coming out of this?

1. The Jakarta Post, "Jokowi wants local governments to ditch Visa, Mastercard", TheJakartaPost, (March 2023).
2. Ricky Mohammad Nugraha and Petir Garda Bhwana, "Jokowi Lauds Domestic Govt Credit Card, International QRIS Launch", TempoCo, (August 2022).
3. Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, especially for the EU", Springer Philosophy & Technology, 33, (2020), pp. 369-378.
4. Julia Pohle and Thorsten Thiel, "Digital Sovereignty", Internet Policy Review – Journal on Internet Regulation, Vol. 9, Iss. 4, (2020), pp. 3.
5. Stephane Couture and Sophie Toupin, "What does the notion of "sovereignty" mean when referring to the digital?", New Media & Society, Vol. 21, Iss. 10, (2019), pp. 2305-2322.
6. Stephane Couture and Sophie Toupin, "What Does the Concept of 'Sovereignty' Mean in Digital, Network and Technological Sovereignty?", GigaNET: Global Internet Governance Academic Network – Annual Symposium 2017, (2018), pp. 2.

THE URGENCY OF DIGITAL SOVEREIGNTY IN INDONESIA AND ITS BENEFITS

As digital sovereignty refers to a nation's ability to maintain control over its digital assets, infrastructure, and data, as well as to protect the digital rights and privacy of its citizen, by having a heavy reliance to international digital services might make the effort to have a secure networks and protection of the digital realm counterproductive. For instance, the digital industries are mainly monopolised by the big tech companies, such as Microsoft, Google, and AWS. In the case that there are data breaches or disputes between parties that must push those service providers to convey its user's data might lead to the leaks of Indonesia's citizen big data into the dark web.

Further, if disputes arise between users and the services, there will be fraction in the implementation of the laws considering that the foreign services still must be in compliance with their national legislations that are disadvantaging its customers who are nationals of foreign countries. Another concern lies within the possibilities of the country involvement to this technology sector that have full control over the digital sphere in times of crises, just like what happened in Russia and Ukraine. The growing and worsening mistrust between nations[7] and heavy reliance on foreign technologies might disabled a whole country's cybersecurity systems that are needed not only for war, but on a day-to-day basis, such as bureaucracy or public health sectors.

Indonesia has seen a considerable increase in cyberattacks and security breaches in recent years. In 2019, Indonesia experienced about 290 million cyberattacks.[8] These dangers include data breaches, financial fraud, cyber espionage, and critical infrastructure assaults, emphasising the need for Indonesia to bolster its digital sovereignty and cybersecurity capabilities. However, the lack of control to its own digital realm might raise the confusion on pinning the blame and who should be made liable on these attacks.

Digital sovereignty is intrinsically linked to innovation and technological advancement since a nation with more control over its digital assets and infrastructure may more effectively promote local enterprises and startups.[9] Strengthening Indonesia's digital sovereignty may assist in establishing an enabling environment for local ICT enterprises, boosting innovation and global market competitiveness. Additionally, fostering technical autonomy and decreasing dependency on foreign digital goods and services may help grow a healthy and self-sufficient digital economy.[10]

INDONESIA'S CURRENT LEGAL AND REGULATORY FRAMEWORK

Indonesia has never made any official statement on aiming into digital sovereignty. However, there are relevant legal frameworks that touch the bases of digital sovereignty.

7. Benjamin Cedric Larsen, The Geopolitics of AI and the rise of digital sovereignty (Brookings Institute 2022).
8. This report is released by Indonesian National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, or BSSN). The number shows a 25% increase compare to the previous year, when cybercrimes had caused losses of USD 34.2 billion for Indonesia. See, Noor Halimah Anjani, "Cybersecurity Protection in Indonesia", Research Report, Policy Brief Number 9, Centre for Indonesian Policy Studies (CIPS), Jakarta.
9. Organisation for Economic Co-operation and Development, Going Digital: Shaping Policies, Improving Lives – Summary, (Paris: OECD, 2019).
10. Jeanette Hofmann, "Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice", Journal of Cyber Policy, Vol. 1, Iss. 1, (2016), pp. 29-49.

1. Law No 11 of 2008 on Electronic Information and Transaction ("ITE Law")
2. Law No. 3 of 2002 on National Defence ("Law on National Defence")
3. Government Regulation No 71 of 2019 on Implementing Electronic Systems and Transactions ("GR 71/2019")

As the umbrella regulation that provides guidance on electronic information and transactions, Article 15 of the ITE Law regulates that any electronic system provider must provide electronic systems in reliable and secure manner and shall be responsible for the proper operation of the electronic systems. This means that all electronic system providers, regardless of whether the system is used for governmental, commercial, or personal purposes, must ensure the operation of the system runs reliably, safely, and responsibly.

Indonesia's Government Regulation Number 71 of 2019 on Implementing Electronic Systems and Transactions (GR 71/2019) replaces Government Regulation Number 82 of 2012 (GR 82/2012). Among the revisions included in the new GR 71/2019 are the following, amongst others:[11]

1. the position of Electronic System Operator has been divided into two classes, which are private domain and public domain; and
2. the electronic system operator's private domain may offshore the administration, processing, and/or storage of electronic systems and data in Indonesia, whilst of public scope should be onshore.

This regulation did not reach the possibility that the providers of the storage or servers might be purchased or subscribed from an international company, which has access to their data control and still have to submit to foreign laws or their company's origin.[12] Further, this GR also lets operators of private scope store data offshore even though it involves the citizen of Indonesia's data, whilst the previous version of this GR mandated whether public and private sector to store data onshore.

Through the Law on National Defence, it can also be presumed that the existing electronic systems in Indonesia are expected to become a unified system that is solid, reliable, and secure nationally. This is in line with the principle of national defence in Article 1 point 1 of the Law on National Defence, that national defence is all efforts to defend state sovereignty, territorial integrity of the Republic of Indonesia, and the safety of the entire nation from threats and disturbances to the integrity of the nation and state. Therefore, the management of electronic systems implemented in Indonesia is also expected to become a national defence effort in building and fostering the capability, deterrence of the state and nation, and overcoming any threat, as stated in Article 6 of the Law on National Defence.

POLICY RECOMMENDATIONS AND STRATEGIES FOR IMPLEMENTATION

There are several policy suggestions and implementation strategies, first, establishing a

11. Article 20 and 21 of the Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions regulates that Electronic Systems Operators of the Public Scope must have a continuity of operations strategy to address disruptions or catastrophes in line with the risk of the resultant consequences. Private Electronic System Operators are permitted to manage, process, and/or store Electronic Systems and Electronic Data inside and/or outside Indonesia. If the Electronic System and Electronic are managed, processed, or kept outside of Indonesian territory, the Private Electronic System Operator is obligated to guarantee the efficacy of monitoring by the relevant Ministries or Agencies and law enforcement. The regulatory and supervisory authorities of the financial industry impose additional regulations on the administration, processing, and storage on Electronic Systems.
12. In the United States, The CLOUD Act was enacted in response to problems the Federal Bureau of Investigation (FBI) encountered in acquiring remote data from service providers through Stored Communications Act (SCA) warrants since the SCA was created before cloud computing was a viable technology. During a 2013 investigation into drug trafficking, the FBI obtained an SCA warrant for emails that a U.S. citizen had stored on one of Microsoft's distant servers in Ireland, but Microsoft refused to comply. This legal dispute led to Microsoft Corp. v. United States before the Supreme Court. The FBI maintained that Microsoft had complete control over the data and should be forced to provide it in response to the demand. However, Microsoft asserted that the SCA did not apply to data housed outside the United States. The challenge acknowledged that while the FBI could request a mutual legal assistance treaty (MLAT) to aid in data discovery during cross-border law enforcement, the process to acquire a new MLAT if one is not already in place or to process a request through an existing MLAT can be time-consuming and hinder law enforcement efforts.

comprehensive national plan for digital sovereignty. This establishment can be implemented through a coordinated approach[13] and linkage with national development objectives.[14] Second, enhancing the legal and regulatory structure through updating existing regulations[15] and establishing new legal frameworks.[16] Third, improving digital infrastructure and the digital ecosystem through increasing broadband connectivity[17] and supporting local technology companies and start-ups.[18] Fourth, enhancing digital literacy and public awareness, which can be undertake through national digital literacy campaigns[19] and integration of digital literacy into the education system.[20] Lastly, promoting international collaboration and cooperation which can be achieved through regional and global partnerships[21] and participations in international forums.[22]

CONCLUSION

Due to rising cyber threats and digital technology dependence, digital sovereignty is a global challenge for countries. Indonesia needs digital sovereignty to maintain national security, economic progress, and social development in the fast-growing digital environment. Increased internet usage, a vibrant technology industry, and expanding investment in digital initiatives show that Indonesia has developed its digital infrastructure and ecosystem. The digital gap, low digital literacy, and the need for a comprehensive legal and regulatory framework to manage developing digital concerns continue. Indonesia must combine national interests with international commerce and obligations to attain digital sovereignty. **(SPU/FNA)**

13. The Indonesian government should design a comprehensive national digital sovereignty policy incorporating input from diverse stakeholders, such as the commercial sector, academia, and civil society. Fulvio Castellacci and Clara Vinas-Bardolet, "Internet Use and Job Satisfaction", Computers in Human Behaviour, Vol. 90, (January 2019), pp. 141-152.
14. The plan should be aligned with Indonesia's more significant economic and social development objectives, ensuring that digital sovereignty activities contribute to inclusive and sustainable progress. See, World Bank, "Ensuring a More Inclusive Future for Indonesia through Digital Technologies", Press Release Number 2022/004/EAP, (2021).
15. Existing rules and regulations should be reviewed and updated to accommodate increasing digital concerns, including data protection, privacy, and security. See, United Nations Conference on Trade and Development, "Digital Economy Report 2019 – Value Creation and Capture: Implications for Developing Countries", UNCTAD, (2019).
16. Novel legal frameworks may be necessary to meet particular digital sovereignty concerns, such as data localisation and cross-border data flows. See, Anupam Chander and Uyen P. Le, "Data Nationalism", Emory Law Journal, Vol. 64, Iss. 3, (2015), pp. 677-739.
17. To bridge the digital gap, the government should prioritise investments in broadband infrastructure, especially in undeserved rural regions. See, World Bank, Op. Cit.
18. The government may aid the creation of local technology enterprises by offering financial assistance, tax benefits, and access to innovation centres and incubators. See, PricewaterhouseCoopers, "Indonesia's Fintech Lending: Driving Economic Growth Through Financial Inclusion", PWC Indonesia – Fintech Series, (2019).
19. The government, in partnership with the commercial sector and educational institutions, should establish a national digital literacy campaign to increase public awareness and enhance digital skills across the population. See, Nancy Law, David Woo, Jimmy de la Torre, Gary Wong, A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2., (Montreal: UNESCO Institute for Statistics, 2018).
20. Digital literacy should be included in the national curriculum at all school levels to ensure students gain the skills essential to flourish in the digital age. See, Organisation for Economic Co-operation and Development, Op. Cit.
21. Indonesia should aggressively participate in regional and global partnerships on digital sovereignty, engaging with other nations to build common norms, standards, and best practices. See, ASEAN, ASEAN Digital Masterplan, (Jakarta: ASEAN, 2020).
22. Indonesia should engage in international forums on digital policy, such as the G20 Digital Economy Task Force and the Internet Governance Forum, to exchange information and learn from other nations. See, G20, "G20 Ministerial Statement on Trade and Digital Economy".

CLOUD-BASED PROCESSING AND DATA PROTECTION LAWS IN INDONESIA

INTRODUCTION

We use cloud-computing, such as Google Drive, Dropbox, and SharePoint in Microsoft 365,[1] on a daily basis. These technologies are used to store data and make it easier for users to share data with other users. Cloud-based processing, also known as cloud computing, allows users to access and utilize remote computing resources through the Internet. In cloud computing, the processing of data, applications, and services is carried out on remote servers located in data centres rather than on the user's own computer or device.

This technology allows users to store, process, and manage data and applications remotely, using a shared pool of computing resources, such as servers, storage devices, and software applications, hosted by a cloud service provider. These resources can be accessed over the internet from anywhere, at any time, using a web browser or specialized software.[2]

There are several advantages to cloud-based processing. One of the main benefits is scalability, as users can easily add or remove computing resources as needed, without the need for expensive hardware or software upgrades. Cloud computing also provides flexibility, allowing users to access their data and applications from anywhere, using any device with an internet connection.[3]

On the other hand, the use of cloud-based processing has significant potential risk. The risk comes particularly in the form of misuse of customer privacy data including confidential business data that can be carried out by governments and cloud-based processing provider companies.

DATA PROTECTION LAWS IN INDONESIA

Initially, regulations regarding Personal Data Protection were regulated in the Ministry of Communication and Information Regulation Number 20 of 2016 concerning Personal Data Protection in Electronic Systems ("MOCIR 20/2016"). Based on Article 1 paragraph (1) MOCIR 20/2016, personal data is defined as certain personal data that is stored, maintained, and maintained truthfully and protected confidentially. This includes but is not limited to, names, addresses, phone numbers, email addresses, biometric data, and financial information. Personal data protection is closely related to the cloud computing system since the cloud is used to store and process vast amounts of personal data of its users. The cloud computing users must also give attention to their personal data and ensure that their cloud service providers implement appropriate security measures and adhere to data protection regulations.

1. https://support.microsoft.com/en-us/office/what-is-sharepoint-97b915e6-651b-43b2-827d-fb25777f446f, accessed on 11 April 2023
2. Witold Maranda et.al, *Data Processing in Cloud Computing Model on the Example of Salesforce Cloud*, Journal Information 2022, 13,85, pg. 5
3. Anca Apostu, et.al, *Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Application in the Cloud*, Recent Advances in Applied Computer Science (RAACS) and Digital Services, ISBN: 978-1-61804-179-1, pg. 120

The law requires data controllers (entities that collect and process personal data) to obtain the consent from individuals before collecting and processing their personal data. Data controllers are also required to implement appropriate security measures to protect personal data from unauthorized access, disclosure, alteration, or destruction.

Indonesia as a developing country has a large number of users of modern technology, based on the statistical data report by Hootsuite (We are Social) there are 204,7 million internet users in Indonesia as of January 2022[4] and communication systems and the government has passed regulations governing the Protection of the Personal Data of Indonesian citizens in Law Number 27 of 2022 concerning Personal Data Protection ("PDP Law"). Article 1 paragraph (2) of Personal Data Protection Law explains that Personal Data Protection is the overall effort to protect personal data and in the course of processing Personal Data, the constitutional rights of Personal Data subjects must not be infringed. The article states that personal data is protected by law as a guarantee of citizens' basic rights. Further, Article 5 of PDP Law states that Personal Data Subjects have the right to obtain information about the clarity of identity, the basis of legal interest, the purpose of requesting and using Personal Data, and the accountability of the party requesting Personal Data.

CLOUD-BASED PROCESSING AND COMPLIANCE WITH DATA PROTECTION LAWS IN INDONESIA

Risk and Challenges

Due to the nature of its function, there are certain risks and challenges associated with cloud-based processing. Some are as follows:[5]

1. Data Security Risks: One of the main risks associated with cloud-based processing is data security. Organizations that use cloud-based processing services are vulnerable to data breaches and cyber-attacks. The risk of data breaches increases if the cloud-based service provider does not implement strong security measures to protect data. Security aspects that need to be considered by a company that implements cloud-based processing, among others: (i) Confidentiality; (ii) Integrity; (iii) Authentication; (iv) Availability; (v) Access Control; (vi) Nonrepudiation.[6]
2. Legal Compliance Risks: Another risk is the failure to comply with legal regulations in Indonesia. Organizations that use cloud-based processing services must comply with data protection laws and regulations to avoid potential legal and financial consequences.
3. Connectivity and Infrastructure Challenges: In Indonesia, infrastructure and connectivity are still developing, and not all areas have access to high-speed internet connectivity. This can pose a challenge for cloud-based processing services, which require a stable and fast internet connection.
4. Data Sovereignty: There is also a risk associated with data sovereignty. If the cloud-based processing service provider is located outside of Indonesia, there may be concerns about the legal jurisdiction and control of the data.
5. Vendor Lock-in: Organizations that use cloud-based processing services are dependent on the cloud service provider, which can lead to vendor lock-in. This can make it difficult to switch to another cloud service provider in the future.

Consequential Obligations

Looking at the risks and challenges, cloud-based data processing comes with the possibility of violations of the use of personal data considering how much data could be processed in its application. These data may fall into the category of personal data as defined in Personal Data Protection Law. The Personal Data Protection Law distinguishes 2 types of personal data.[7] The first is specific personal data which consists of health data and

4. https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2022/, accessed on 10 April 2023
5. Joni, dkk, *Mitigation of The Risk of Cloud Computing*, ULTIMA InfoSys, Vol. X No. 2, 2019, pg. 100
6. Munirul Ula, *Analisis Metode Pengamanan Data Pada Layanan Cloud Computing*, TECHSI: Vol.11 No. 1, 2019, pg. 128-132

information, biometric data; genetic data; criminal record; child data; personal financial data; and/or other data in accordance with the provisions of laws and regulations. The second type is personal data of a general nature. It consists of full name; gender; citizenship; religion; marital status; and/or personal data combined to identify an individual.

Personal Data Protection Law regulates the parties involved in the processing of Personal Data, namely the Personal Data Controller and the Personal Data Processor. A Personal Data Controller is any person, public body and international organization acting individually or jointly in determining the purposes and exercising control over the processing of Personal Data.[8] Meanwhile, a Personal Data Processor is any person, public body and international organization acting individually or jointly in carrying out the processing of Personal Data on behalf of the Personal Data Controller.[9]

In the universe of cloud computing systems, personal data controllers can be interpreted as individuals or companies using cloud services to whom the rights are attached to determine the purpose of use and control the data stored in the cloud system. Meanwhile, personal data processors can be interpreted as a cloud-based technology provider company that performs processing of data owned by personal data controllers.

Consequently, cloud computing users – in this case, personal data controllers, must ensure that their cloud services providers implement appropriate security measures. The security measures can be interpreted as personal data protection obligations that must be fulfilled by the personal data controller. Some of the obligations referred to for the Personal Data Controller are listed in several Articles, as follows:[10]

1. Must have a basis for processing Personal Data;
2. Required to process Personal Data must carry out limited and specific processing of Personal Data;
3. Obliged to carry out the processing of Personal Data in accordance with the purpose of processing Personal Data;
4. Must ensure the accuracy, completeness and consistency of personal data in accordance with the provisions of laws and regulations;
5. Must record all personal data processing activities;
6. Must protect and ensure the security of personal data processed;
7. Must maintain the confidentiality of personal data in processing personal data;
8. Shall supervise any party involved in the processing of personal data under the control of the personal data controller;
9. Shall protect personal data from unauthorized processing;
10. Must prevent personal data from being accessed unlawfully;
11. Must be responsible for the processing of personal data and show responsibility in fulfilling obligations to implement the principles of personal data protection;
12. Must appoint an official or officer who carries out the function of Personal Data Protection;

Potential Sanctions

Furthermore, as described above, one of the main risks in using cloud-based technology is regarding the security of users' personal data. Therefore, PDP Law in this case has sufficiently regulated comprehensively the prohibition on the use of personal data and sanctions or penalties for violations of the use of personal data as stipulated in Articles 65 to Article 73 of the Personal Data Protection Law. More specifically, regarding violations related to personal data, such as obtaining,

7. Article 4 of PDP Law
8. Article 1 point 4 of PDP Law
9. Article 1 point 5 of PDP Law
10. Article 20 paragraph (1), Article 27, Article 28, Article 29, Article 31, Article 35, Article 36, Article 37, Article 38, Article 39, Article 47, Article 53 of PDP Law

collecting, disclosing, using personal data unlawfully which can cause harm is further regulated in criminal provisions in Article 67 of PDP Law, which reads:

> "Article 67
> Any Person who deliberately and unlawfully obtains or collects Personal Data that is not his own with the intention of benefiting himself or another person which can result in loss of the Personal Data Subject as referred to in Article 65 paragraph (1) shall be punished with imprisonment for a maximum 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah).
>
> Any Person who deliberately and unlawfully discloses Personal Data that does not belong to him as referred to in Article 65 paragraph (2) shall be subject to imprisonment for a maximum of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000. 00 (four billion rupiah).
>
> Any Person who deliberately and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3) shall be subject to imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000. 00 (five billion rupiah)."

Broadly, the Personal Data Protection Law can provide a deterrent effect to personal data violators. However, the Personal Data Protection Law should reduce the number of people involved in personal data breach cases, especially in this case are people and companies that implement cloud-based processing in their work systems.

Overall, while cloud-based processing offers many benefits, organizations in Indonesia must carefully consider the risks and challenges associated with this technology prior to implementing it. They should also ensure that they choose a reputable and reliable cloud service provider that is compliant with the Personal Data Protection Law as a legal umbrella of for managing and protecting citizens' data, including the users of cloud computing.

CONCLUSION

Indonesia has passed the Personal Data Protection Law as a regulation on personal data protection with more extensive and detailed provisions that are expected to minimize violations of the use of personal data, especially cloud-based processing users. However, issues of concern regarding the use of personal data also need to be considered by the company that implements the system. In addition, cloud computing providers who are in the public sphere are required to manage, process, and/or store electronic data in the territory of Indonesia, meaning that cloud computing service providers are required to have a data center in Indonesia. This is because the working domain of cloud computing providers is in the public domain and these data concern the sovereignty of Indonesian citizens.

By further regulating the obligations of personal data subjects which also include companies that use cloud computing systems to which personal data from a company are attached, further regulation regarding violations of personal data is expected to become a benchmark and provide awareness to companies using cloud computing and cloud computing provider. **(IAN/FMN/EFF)**

CAN ARTIFICIAL INTELLIGENCE FINALLY SUBSTITUTE THE LEGAL PROFESSION?

INTRODUCTION

Gustav Radburch in delivering his doctrine on the ideals of law (idee des recht) stated that the law enforcement process should fulfil 3 (three) main principles, namely the principles of legal certainty, justice and expediency.

In law enforcement practice, the three legal principles cannot always be applied simultaneously. For instances, in context of ensuring the principle of justice, the Constitutional court in its consideration for Decision Number 33/PUU-XIV/2016 has declared that the principle of justice shall take precedent over the principle of legal certainty, specifically in criminal cases, where efforts to find justice shall not be restricted by time. This is in contrast with the efforts to achieve legal certainty by fixing a time frame within which to commence a criminal action.

Indonesia, as with any other modern State, has a legal system that must provide for the enforcement of its laws through law enforcements professionals, i.e., Judges, Prosecutors and Advocates. Each professional has rights and obligations as well as specific authority and responsibility in the legal system and these are stipulated in the laws and regulations for each of the professions.

THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGY IN THE LAW

With the rapid development of technology in the recent years, humas has succeeded in creating Artificial Intelligence ("AI") which assist and facilitate human affairs, e.g., the popular Siri virtual assistant technology applied in iPhone, will help find an address or orally remind the user of a scheduled meeting.

In its journey, AI has specifically penetrated into the law enforcement profession, such as:

1. February 2019, in Canada a "robot mediator" succeeded to settle a court case for the first time. By utilizing Smartsettle ONE □ an online dispute resolution (ODR) tool developed in British Columbia which employs algorithms that learn the bidding tactics and priorities of the parties to a dispute and helped move them towards a settlement.[1]

2. March 2019, Estonian Ministry of Justice proposed for "Ott Velsberg" (Government Chief Data Officer of Estonia) to design a "robot judge" that could adjudicate small claims disputes of less than €7,000.[2]

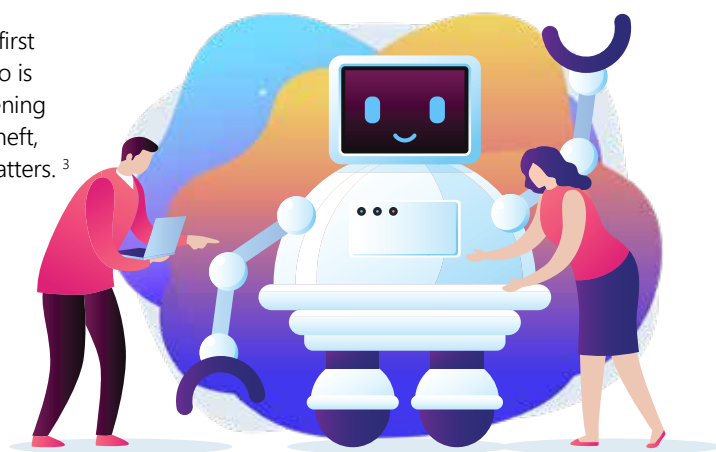
3. December 2021, China became the world's first country to make an AI-equipped judge, who is said to give 97% correct decisions after listening to oral arguments. These judges can hear theft, credit card fraud, and dangerous driving matters. [3]

4. On 30 January 2023, Judges in Colombia rendered a final decision for a dispute with the health insurance company by using ChatGPT to ask questions on whether an autistic child should receive coverage for medical treatment, which the AI decided in favour of the autistic child.[4]

PROS AND CONS OF USING AI

The use of AI has its pros and cons. AI has fewer errors than humans. AI runs 24/7 without needing a break (as long as the power is turned on). AI can analyze massive amounts of data in a shockingly small amount of time compared to the human. On the other hand, AI is generally considered to lack creativity and innovative ways for solutions. AI can also be a threat to humans by increasing unemployment. Lastly, as AI is purely logical, it is very difficult to incorporate areas such as ethics and morality into the algorithm.[5]

In the context of law enforcement, the controversy is whether the judiciary can rely on AI. The AI-Lawyer or AI-Mediator do not expose the judicial system nor the parties to unnecessary risk, as there is always a human judge to check and verify the AI rendered decision. It is worth remembering that a human judge's role is complex and sensitive. Leaving it purely to an algorithm is viewed with scepticism. It is necessary to set a boundary between technology and humans.



1. Tara Vasdani, "From Estonian AI Judges to Robot Mediators in Canada, U.K.", 13 June 2019, accessed from From Estonian AI judges to robot mediators in Canada, U.K. | LexisNexis Canada.
2. Tara Vasdani, "Estonia set to introduce 'AI Judge' in Small Claims Court to Clear Court Blacklog", 10 April 2019, accessed from https://www.law360.ca/articles/11582/estonia-set-to-introduce-ai-judge-in-small-claims-court-to-clear-court-backlog-
3. Morning Express, "China Made the World's Firsts Artificial Intelligence-Equipped Judge, Gives 97 percent of the Decisions Right", 28 December 2021, accessed from https://morningexpress.in/china-made-the-worlds-first-artificial-intelligence-equipped-judge-gives-97-percent-of-the-decisions-right/
4. VOI, "Judges in Colombia Use ChatGPT To Make Court Decisions, The Result?", 4 February 2023, accessed from https://voi.id/en/amp/251021
5. Forbes, "The Pros and Cons of Artificial Intelligence", 1 December 2022, accessed from https://www.forbes.com/sites/qai/2022/12/01/the-pros-and-cons-of-artificial-intelligence/amp/

AI REGULATION IN INDONESIA

Currently Indonesia has no AI-specific laws nor regulations. But the concept of AI can be equated as an "Electronic Agent"[6] namely a device of an Electronic System that is designed to perform any action. This is described in in Law Number 11 of 2008 concerning Information and Electronic Transaction ("UU ITE").

If the doctrines of the ideals of law conveyed by Gustav Radburch is connected to the role and function of Judges, Prosecutors and Advocates as professionals and law enforcement institutions that are responsible for achieving the principle of legal certainty, justice, expediency, therefore AI could not replace the legal profession, considering:

1. AI is not a legal subject who can bear a right and obligation unlike Judges, Prosecutors and Advocates, and cannot be attached to legal authority and responsibility as a logical consequence of legal profession;

2. AI as a technology system could not stand alone but requires a "human" role in its operation, referring to UU ITE, it is known that Electronic Agents are the parties responsible for all legal consequences carried out by AI and Electronic Agents does not necessarily have a background in the legal field. Therefore, AI as a system is not recognized as an independent legal subject under Indonesian law; [7]

3. AI is entirely dependent on the data stored in its database, and is not intended to make an assessment of something that is outside the database; Thus, in concrete cases, AI cannot be left to judge whether a fact has fulfilled the sense of justice or not;

Based on the description above, by looking at the nature and function of AI as a system controlled by Electronic Agents, it can be concluded that the position of AI is only as a tool of the law enforcement profession such as Judges, Prosecutors and Advocates and cannot replace their functions.

In addition, the newly developed technology should only be considered assistance, never as a substitute for a human judge. Therefore, to understand this, it is important to draw a comparison between the conceptual abilities of technology and humans.[8] **(DBS/FJM)**

6. Zahrashafa P.M., Angga P., "Pengaturan Hukum Artificial Intelligence Indonesia Saat Ini", accessed from https://law.ui.ac.id/pengaturan-hukum-artifical-intelligence-indonesia-saat-ini-oleh-zahrashafa-pm-angga-priancha/
7. Arudanti S. W., "Wamenkumham: AI Sulit Dikategorikan Sebagai Subjek Hukum", 15 October 2021, accessed from https://www.cloudcomputing.id/berita/wamenkumham-ai-sulit-dikategorikan-subjek-hukum.
8. Aditya Gatlewar, "Emergence of a New Dimension to the Judicial System: AI – A Threat or Boon", accessed from https://disputescentre.com.au/emergent-of-a-new-dimension-to-the-judiciary-system-ai-a-threat-or-boon/

THE FUTURE OF EDUCATION: BRIDGING THE GENDER GAP IN TECHNOLOGY SKILLS

INTRODUCTION

The exponential rate of digital change has resulted in a fundamental shift in the contemporary workforce, with technological skills becoming more important across sectors and job functions.[1] As organisations and companies become increasingly dependent on digital tools and processes, there is a rising need for personnel who can successfully utilise, create, and manage technology to fulfil organisational objectives and maintain global market competitiveness.[2]

From fundamental digital literacy, such as the ability to operate software and online platforms,[3] to more sophisticated abilities, such as programming, data analysis, and cybersecurity, technology skills comprise a broad spectrum of proficiencies.[4] These competencies are no longer restricted to conventional technology-related disciplines, as they have become indispensable in various industries, including banking, healthcare, education, and even law.[5] The growing dependence on technology in practically every facet of professional life underscores the need to prepare the workforce to traverse the digital terrain.[6]

The increased focus on science, technology, engineering, and mathematics (STEM) education and incorporating digital literacy and technology training into school curricula results from the demand for technological skills in the contemporary workforce.[7] As technology progresses and infiltrates different sectors of society, persons with solid

1. Klaus Schwab, The Fourth Industrial Revolution, (Cologny: World Economic Forum, 2016), pp. 14.
2. Centre for the New Economy and Society, "The Future of Jobs Report 2018", Insight Report, World Economic Forum, (2018).
3. Pew Research Center, "The State of American Jobs", Report, (2017).
4. Jacques Bughin, Eric Hazan, Susan Lund, Peter Dahlstrom, Anna Wiesinger, Amresh Subramaniam, "Skill shift: Automation and the future of the workforce", Discussion Paper, McKinsey Global Institute, (May, 2018).
5. Ibid.
6. Centre for the New Economy and Society, Op. Cit.
7. Diane L. Souvaine, et. al., "The State of U.S. Science and Engineering 2020", Report, National Science Board – Science & Engineering Indicators, (2020).

technological skills are better positioned for job success and advancement,[8] whilst those without such abilities may have restricted options and risk falling behind.[9]

Considering the significance of technological skills in today's industry, it is crucial that all persons, regardless of gender, have equal access to the necessary resources, opportunities, and assistance to acquire these abilities. Bridging the gender gap in technological skills not only promotes social justice and gender equality[10] but also adds to a more diversified, inventive, and competent workforce in the digital era.[11]

THE GENDER GAP IN TECHNOLOGY SKILLS

Women are underrepresented in technological education and employment globally. The World Economic Forum's 2020 Global Gender Gap Report found that just 32% of higher education STEM students are female.[12] According to the study, women hold 28% of STEM jobs globally. In 2016–2017, women earned 19% of bachelor's degrees in computer science and 20% of engineering degrees in the US, according to NCES.[13] Women make up 26% of computer science and mathematics workers and 14% of architectural and engineering workers in the US, according to the BLS.[14] East, South, and Southeast Asia have 23% female STEM researchers, according to the UNESCO Institute of Statistics.[15] Many factors complicate the gender gap in technology education and employment; societal expectations and misconceptions, lack of access to resources and opportunities, and a dearth of female role models in technical fields keep this disparity alive.

Societal norms and gender stereotypes exacerbate the technical skills gap between men and women. These conventions and beliefs shape boys' and girls' talents, interests, and career possibilities early on. Research suggests that stereotypes of technology and STEM disciplines as masculine, may hurt women's confidence and willingness to work in these fields.[16] Studies show that girls as young as six are less inclined than boys to regard their gender as "really, really intelligent" and avoid activities marketed to "brilliant" kids.[17] Internalising gender stereotypes may dissuade girls from pursuing STEM fields like technology and perpetuate the underrepresentation of women in these fields.

The lack of access to resources and opportunities for girls and women is another crucial factor in the gender gap in technological skills. This discrepancy is noticeable in many areas, including access to education,[18] technology,[19] mentoring,[20] money,[21] and socioeconomic issues.[22] To overcome these obstacles, governments and non-governmental organisations must invest in infrastructure and programs targeting

8. Centre for the New Economy and Society, Op. Cit.
9. Pew Research Center, Op. Cit.
10. United Nations, "Transforming Our World: the 2030 Agenda for Sustainable Development", General Assembly, A/Res/70/1, (2015).
11. Centre for the New Economy and Society, Op. Cit.
12. World Economic Forum, "Global Gender Gap Report 2020", Insight Report, (2020).
13. National Centre for Education Statistics, "Digest of Education Statistics", Report, (2019).
14. U.S. Bureau of Labor Statistics, "Labor Force Statistics from the Current Population Survey", Survey, (2022).
15. UNESCO Institute for Statistics, "Women in Science", Fact Sheet, United Nations Educational, Scientific, and Cultural Organisation, Number 51, (June 2018), FS/2018/SCI/51.
16. Sapna Cheryan, Allison Master, and Andrew N. Meltzoff, "Cultural stereotypes as gatekeepers: increasing girls' interest in computer science and engineering by diversifying stereotypes", Frontiers in Psychology – Hypothesis and Theory Article, Vol. 6, Art. 49, (February 2015).
17. Lin Bian, Sarah-Jane Leslie, Andrei Cimpian, "Gender stereotypes about intellectual ability emerge early and influence children's interests", Research Report, Science, 355 (6326), pp 389-391.
18. Females are often underrepresented in STEM fields owing to many problems, such as biased teaching techniques, insufficient learning resources, and a need for more female role models. See, UNESCO, Cracking the code: girls' and women's education in science, technology, engineering and mathematics (STEM), (Paris: The United Nations Educational, Scientific and Cultural Organisation, 2017), pp. 19.
19. The digital divide disproportionately affects girls and women, defined as the difference between those with access to digital technology and those without. See, World Bank Group, "Accelerating Gender Equality in Digital Development", (November 2021). This digital gap must be bridged by providing poor areas with inexpensive, dependable internet connections and digital gadgets.
20. Often, women in technology need extra mentoring and networking opportunities, which might impede their career advancement. See, Suzanne de Janasz and Beth Cabrera, "How Women Can Get What They Want in a Negotiation", Harvard Business Review, (2018).
21. According to a 2018 report by Boston Consulting Group, female-led businesses obtain less than half the financing of their male counterparts while producing more profits. See, Katie Abouzahr, Matt Krentz, John Harthorne, and Frances Brooks Taplett, "Why Women-Owned Startups Are a Better Bet", Boston Consulting Group, (2018).
22. Socioeconomic constraints exacerbate girls' and women's lack of access to resources and opportunities. See, UNESCO, Op. Cit.

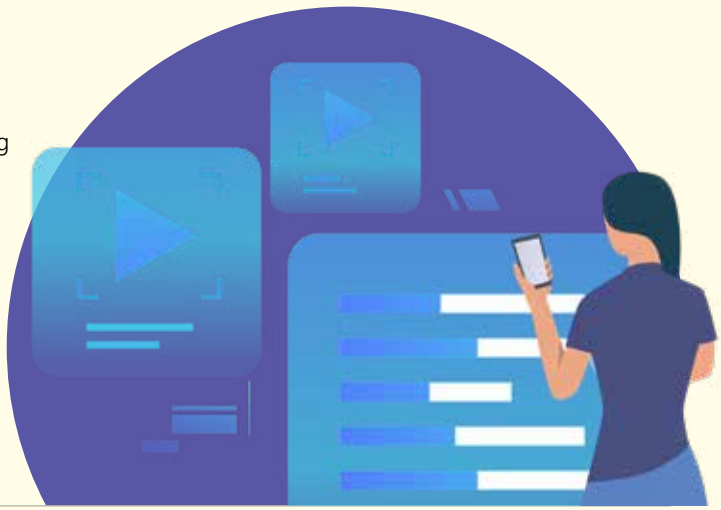
disadvantaged areas to ensure that girls and women have equal access to education.

Another factor contributing to the technology gender gap is the lack of female role models.[23] Girls and women are interested in technological careers whose objectives, self-confidence, and belonging are affected by the portrayal.[24] In conclusion, bridging the gender gap in technical skills requires addressing the lack of female role models in technology-related fields. Increasing the visibility of women in technology, mentorship, specialised training, and inclusive workplaces may help create a more diverse and capable technology workforce.

INCLUSIVE INSTRUCTIONAL STRATEGIES

By moulding children's attitudes, beliefs, and pursuits, early education promotes gender equality in technological skills.[25] Incorporating technology and STEM-related courses without regard to gender in early school may promote a pleasant and inclusive atmosphere that helps girls and boys to develop technological skills and interests.[26]

There are several methods for establishing inclusive educational settings. Firstly, by creating a gender-sensitive curriculum may assist in combating prejudices and biases that contribute to the technological skills gap between men and women.[27] Secondly, promoting cooperation and peer support through a collaborative and supportive learning environment.[28] This may promote gender equality in technological skills.[29] Third, by increasing exposure to female role models in the realm of technology. This effort might help overcome preconceptions and encourage females to seek employment in technology-related fields.[30] Educators may demonstrate to young girls that they, too, can thrive in technology-related industries by inviting outstanding women in



23. Girls may not perceive themselves as represented in STEM fields if there are few famous female role models. See, Sapna Cheryan, Sianna A. Ziegler, Amanda K. Montoya, Lily Jiang, "Why Are Some STEM Fiels More Gender Balanced Than Others?" Psychological Bulletin, (2016). Female role models may make technological careers more appealing to girls. Media, events, and instructional tools may help solve this issue by highlighting women in IT. See, Benjamin J. Drury, John Oliver Siy, Sapna Cheryan, "When Do Female Role Models Benefit Women? The Importance of Differentiating Recruitment From Retention in STEM", Psychological Inquiry – An International Journal for the Advancement of Psychological Theory, Vol. 22, Iss. 4, (2011), pp. 265-269.
24. Connecting girls to female role models in technical fields may help overcome this obstacle. See, Jill Denner, Linda Wener, Steve Bean, and Shannon Campe, "The Girls Creating Games Program", Frontiers: A Journal of Women Studies, Vol. 26, No. 1, (2005), pp. 90-98. Women's underrepresentation in technical fields may create a hostile or biased work environment. See, Sapna Cheryan, Sianna A. Ziegler, Amanda K. Montoya, Lily Jiang, "Why Are Some STEM Fields More Gender Balanced Than Others?", Op. Cit.
25. Allison Master, Sapna Cheryan, and Andrew N. Meltzoff, "Computing Whether She Belongs: Stereotypes Undermine Girls' Interest and Sense of Belonging in Computer Science", Journal of Educational Psychology, Vol. 108, No. 3, (2016), pp. 424-437.
26. UNESCO, Op. Cit.
27. Jacob Clark Blickenstaff, "Women and science careers: leaky pipeline or gender filter?", Gender and Education, Vol. 17, Iss. 4, (2005), pp. 369-386. By including information that challenges gender conventions and promotes the accomplishments of women in technology, educators may nurture the interest of both girls and boys in technology-related courses by creating a more inclusive learning environment. See, Catherine Hill, Christianne Corbett, Andresse St. Rose, Why So Few? Women in Science, Technology, Engineering, and Mathematics, (Washington DC: AAUW, 2010), pp. 93.
28. Fostering group work, peer mentorship, and establishing chances for girls and boys to collaborate on technology-related projects may lead to a more inclusive atmosphere where students feel encouraged to pursue technological skills. See, Stephanie Holmes, Adrienne Redmond, Julie Thomas, Karen High, "Girls Helping Girls: Assessing the Influence of College Student Mentors in an Afterschool Engineering Program", Mentoring & Tutoring: Partnership in Learning, Vol. 20, Iss. 1, (2012), pp. 137-150.
29. Jill Denner, Linda Werner, Eloy Ortiz, "Computer games created by middle school girls: Can they be used to measure understanding of computer science concept?", Computers & Education, Vol. 58, Iss. 1, (January 2012), pp. 240-249.
30. David M. Marx, Jasmin S. Roman, "Female Role Models: Protecting Women's Math Test Performance", Personality and Social Psychology Bulletin, Vol. 28, Iss. 9, (2002).

technology to speak to students, organising field visits to technology businesses, and integrating tales of women's accomplishments into the curriculum.[31]

FUTURE DIRECTIONS AND SUGGESTIONS

To address these issues, several measures can be taken. First, governments and schools should invest in technical education, including modern resources and infrastructure. This requires updating the curriculum, educating teaches, and providing technical resources to all pupils, regardless of gender.[32] Second, encourage technological diversity and inclusiveness. This includes gender-neutral recruiting, mentorship, and career advancement initiatives. Finally, school-NGO-business relationships may benefit all sides. Collaborations may provide access to resources, expertise, and networks, narrowing the gender gap in technology abilities.[33]

Eliminating the gender gap in technical abilities may have long-term benefits, even if it takes time. Second, closing the gender gap in technical skills may boost economic growth and innovation by expanding the talent pool and fostering diverse perspectives on technology development.[34] Closing the technological skills gap may also promote gender equality and social justice by giving women equal opportunities to participate in and benefit from technical advances. Bridging the gender gap in technical skills may also improve legal diversity and competence. This would help the digital justice system better represent and understand diverse viewpoints.

Educational institutions, governments, non-governmental organisations, and businesses must work together to close the technology skills gap. Following policy recommendations and encouraging collaboration may lead to economic growth, gender equality, and more diverse and skilled legal personnel. These actions will promote digital equality and inclusion. **(SPU)**

31. Jane G. Stout, Nilanjana Dasgupta, Matthew Hunsinger, Melissa A. McManus, "STEMing the Tide: Using Ingroup Experts to Inoculate Women's Self-Concept in Science, Technology, Engineering and Mathematics (STEM)", Journal of Personality and Social Psychology, Vol. 100, No. 2, (2011), pp. 255-270.
32. UNESCO, Op. Cit.
33. World Bank, Op. Cit.
34. World Economic Forum, Op. Cit.

TIPS ON COMMUNICATION EXCHANGE TO MITIGATE DATA MISUSE

Today, technological developments have immensely facilitated communication between humans. Communication is carried out not only face-to-face or via telephone and SMS, but also through social media platforms. The use of social media, which are increasingly diverse as a means of communication is not only used by young people but also by adults.[1] However, in its use, there is a risk of problems that may arise, such as misuse of personal data. Based on Article 4 of Law Number 27 of 2022 concerning Personal Data Protection ("Law 27/2022"), personal data consists of:

1. Specific personal data
   a. Health information
   b. Biometrics
   c. Genetics
   d. Criminal record

1. Center for Research and Development of Informatics and Public Information and Communication Applications. 2017. Survey of ICT Use and Its Implications for Socio-Cultural Aspects of Society. Ministry of Communication and Information of the Republic of Indonesia.

e. Children data
f. Personal finance, and
g. Any other data in accordance with the regulation.

2. General personal data:
   a. Full name
   b. Gender
   c. Nationality
   d. Religion
   e. Marital status, and
   f. Other personal data combined to identify an individual.

The government through Law 27/2022 has provided protection for personal data by granting rights to personal data subjects and restrictions on personal data controllers.[2] But it would be even better if the social media users themselves also took mitigation steps to protect their personal data from misuse during the process of communicating on social media. The following are strategies to mitigate the misuse of personal data:

1. **Ensure that the social media platforms used for communication are registered with the Ministry of Communication and Information**
   This aims to ensure that social media platforms are under the supervision of the Ministry of Communication and Information. Thus, the potential for misuse of personal data could be minimized.

2. **Learn the privacy policy on social media**
   Before using social media to communicate, it would be better if users paid closer attention to the privacy policies that have been determined by the social media platform and the purpose of using the personal data information.

3. **Do not give personal data to the interlocutor easily**
   In communicating with the interlocutor, it is important not to give personal data easily. It is necessary to pay close attention to the purpose of sending personal data. This is to avoid any misuse of personal data by both the interlocutor and the social media itself as the access controllers.

4. **Looking for information about the latest crime or misuse of data modes**
   Unfortunately, technological developments have also been followed by developments in the methods used to lure users into submitting personal data through social media. Therefore, it is important to expand our knowledge concerning the latest criminal methods of operation or techniques. Our vigilance as social media users are maintained, and we are not caught off guard by the latest criminal methods.

(JMS/KBA)

2. Pursuant to Article 1 Paragraph 4 of Law 27/2022, controllers of personal data are every person, public agency and international organization that acts individually or jointly in determining purpose and exercising control over the processing of personal data.

www.ap-lawsolution.com

TENDEAN SQUARE KAV. 17-18
Jl. Wolter Monginsidi No. 122-124
Kebayoran Baru, South Jakarta
Indonesia – 12170

PHONE : +62-21-72787678, 72795001
FAX : +62-21-7234151
EMAIL : connect@ap-lawsolution.net