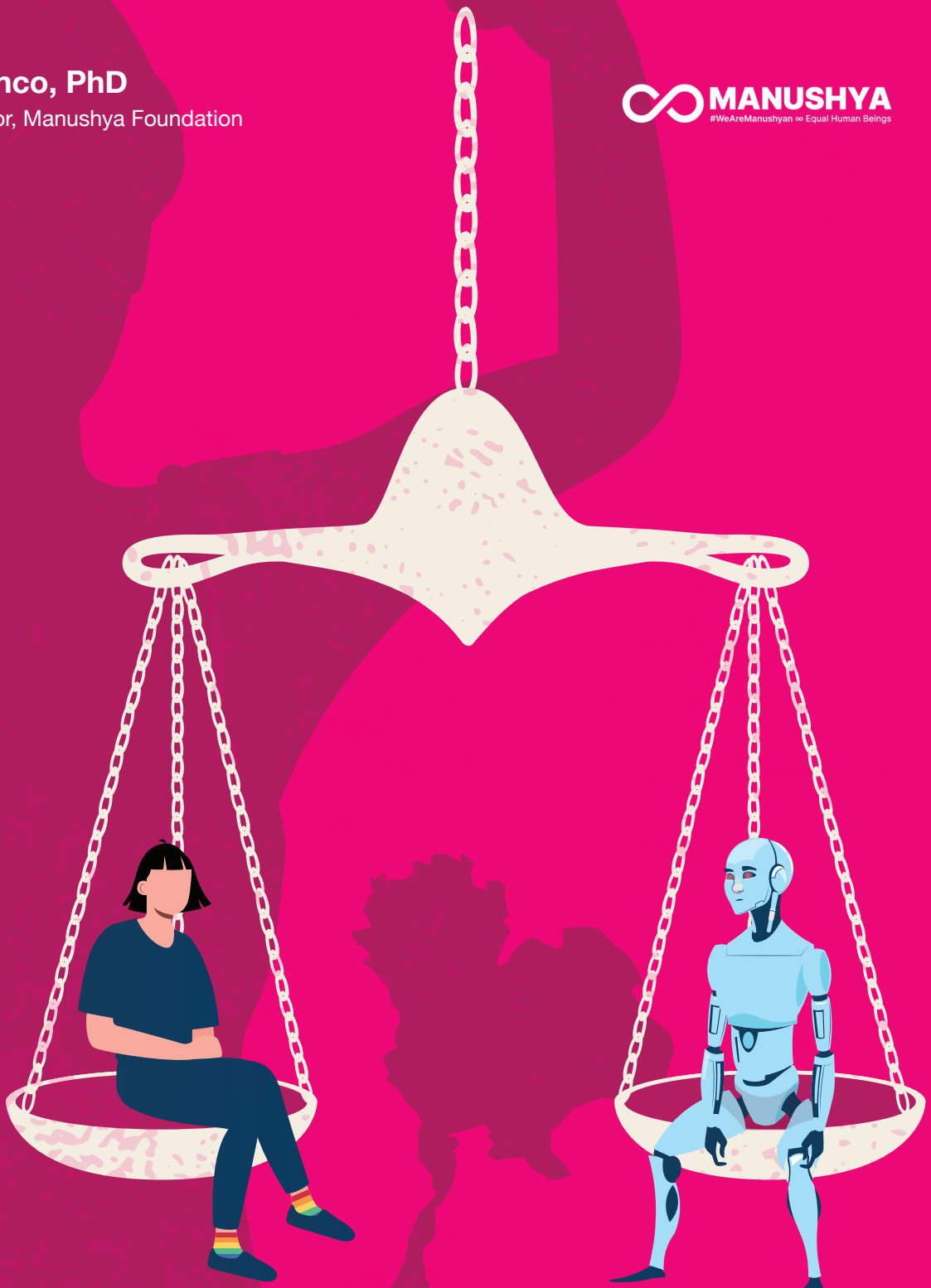
Jean Linis-Dinco, PhD
Digital Rights Advisor, Manushya Foundation

MANUSHYA
#WeAreManushyan ∞ Equal Human Beings



Balancing progress and human rights: Is Thailand ready for Artificial Intelligence that respects human rights?

With pro bono connection from

Acknowledgements

Manushya Foundation and the Thomson Reuters Foundation extend their deepest gratitude to all those who offered unwavering support and unique insights into the digital rights situation in Thailand, contributing to the completion and success of this report.

We would like to express particular appreciation to Manushya's Democracy & Digital Rights Team for their coordination, review, editing, and finalisation of the report. Our heartfelt thanks go to Dr. Jean Linis-Dinco, Digital Rights Advisor at Manushya Foundation, who authored the report, and to Emilie Palamy Pradichit, Founder & Executive Director at Manushya Foundation, whose vision and oversight made this project possible. We are also sincerely grateful to Joanita Britto Menon, Legal Programme Manager, Asia, and Emmanuele Marie C. Parra, Programmes Officer, Asia, at TrustLaw, Thomson Reuters Foundation, for their invaluable support and contributions.

Manushya Foundation and the Thomson Reuters Foundation also acknowledge and extend their gratitude to the law firms who generously contributed their time and expertise on a pro-bono basis to support the legal analysis in the US and Thailand.

The report's graphics and illustrations would not have been possible without the talent and dedication of our designers. We extend our gratitude to Putu Deoris for his meticulous work on the overall layout and design.

Finally, we offer special thanks to our former team researchers and interns at Manushya Foundation for their significant contributions to desk research and the compilation of a Thailand-AI-related depository that informed this report. We are particularly grateful to Letitia Visan, Felicity Salina, and Dissarin Tovikkai for their dedication.

Disclaimer

This report is offered for informational purposes only and does not constitute legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances. While we strive to ensure the report's contents are accurate and up to date at the time of publication, we do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. Manushya Foundation and the Thomson Reuters Foundation accept no liability or responsibility for actions taken or not taken, or any losses arising from reliance on this report or any inaccuracies herein. Similarly, the Thomson Reuters Foundation is proud to support their TrustLaw member, Manushya Foundation, with their work on this report, including its publication and the pro-bono connection that facilitated the legal research. However, in accordance with the Thomson Reuters Trust Principles of independence and freedom from bias, the Foundation does not take a position on the contents of or views expressed in this report.

Dedication

We envision that this report would serve as a benchmark for future studies to provide a more nuanced analysis on the impact of technology in Thai society. This report is just one of the many that Manushya Foundation aims to publish in relation to the impact of emerging technologies on the rights and welfare of the Thai people. Through this report, we ensure that the working class remains at the forefront of every topic and discussion that we put our hearts into. Manushya Foundation will be at the forefront of this battle that would challenge capitalist structures and support the rights and autonomy of the working class in the face of a rapidly changing world.

This study is dedicated to the struggles of the working class whose rights and dignity have been trampled by the relentless capitalist pursuit of profit and influence. We call on the Thai government to ensure that all policies respect and fulfil the human rights of all, not just the selected few.

About Us

Manushya Foundation

Founded in 2017 with the vision to build a movement of Equal Human Beings ∞ #WeAreManushyan ∞ Manushya Foundation is an **Asian Intersectional Feminist human rights organisation reinforcing the power of Humans,** in particular feminists, women, youth, democracy activists, LGBTIQ+ people, indigenous & forest communities, climate and environmental defenders to speak truth to power at the forefront of their fight for Democracy, Social Justice & Equality. Manushya Foundation works at the intersection of democracy and digital rights, corporate accountability and climate justice, and protection and access to justice to ensure that communities are at the heart of decision-making, powering feminist leadership, and resourcing human rights activists and movements. As part of our democracy and digital rights portfolio, our collective goal is to decolonise and decentralise the digital rights field, **amplifying voices** from the ground, following an **intersectional feminist approach**, fearlessly sharing our truths, with focus on **Global Majority voices and class struggles**, including Women, LGBTIQ+ folks, youth, democracy defenders, and marginalized communities, such as indigenous peoples, people with disabilities, and religious minorities (Malayu Muslims and the Rohingya people).

Table of Contents

Table of Tables and Figures

Executive Summary:

Thailand has made significant investments on emerging technologies such as machine learning and Artificial Intelligence. In line with the country's goal of enhancing its economic competitiveness in the international scale, the government prioritised the rapid development of infrastructure and data capabilities.

This move has been widely acknowledged as a step-forward for the middle-income Asian country. Nonetheless, there have been instances of oversights regarding the potential risks that the adoption of this technology may bring. As is often the case, the rapid economic and technological makeover has raised significant concerns about its impacts on the working class and marginalised communities. As such, we would like to open an important point of enquiry. Should economic priorities come at the expense of safeguarding people's rights? And has Thailand implemented necessary regulations to ensure that AI is governed in a way that serves the best interests of its citizens?

This study examines Thailand's AI landscape through the lens of human rights. We use a novel approach to analysing policies through the adoption of Human Rights-focused Policy Impact Assessment (HR-PIA). HR-PIA moves away from the traditional approach of policy impact assessment by putting human rights at the forefront of the investigation instead of an afterthought. This means that policies are judged and probed first based on their human rights impact before anything else. This kind of examination aims to explore how Thailand is using AI for societal benefit while navigating the impact it poses to individuals and the broader community. In this report, we hope to examine whether Thailand is truly equipped to harness the benefits of this technology without trampling on human rights and people's welfare.

It is not a secret that existing laws in the country do not provide sufficient legal protection for individuals affected by AI technologies. In fact, a closer look at the scope of Thailand's data protection legislation shows noticeable shortcomings. The most obvious of these is the lack of specificity when it comes to machine learning and automation use cases. Additionally, the laws also do not apply to data collection conducted by state or public authorities for purposes related to maintaining national security or public safety, which leave room for privacy breaches to occur within contexts that the government deems fit. With all these in mind, there is a pressing need for substantial reforms in both criminal and civil laws. We call for establishing clear legal standing and accountability for AI systems and their creators. This means that human rights-focused policy impact assessment must be done before every deployment and not only act as an ex-post mechanism. We also call for the creation of a robust and independent judicial system that would manage cases involving harm caused by AI.

This report recommends passing a dedicated AI law as part of Thailand's National AI Strategy. At the minimum, the law should be human-centred and should prioritise the rights and well-being of individuals who use technology and may be affected by it. Thailand should also address governance issues related to privacy and data protection to close gaps that may facilitate harmful AI practices. Any attempt to introduce the new AI law must be done with utmost transparency. It should involve the public, civil society and academics and must go beyond mere consultations alone. Shifting the focus towards human rights-based approach to AI development will alleviate the challenges associated with ensuring regulatory compliance in the future.

Acronyms

AI	Artificial Intelligence
AIGC	AI Governance Clinic
ASEAN	Association of Southeast Asian Nations
CICC	Centre of the International Cooperation for Computerisation
CV	Computer Vision
ETDA	Electronic Transactions Development Agency
GOT	Government of Thailand
ICT	Information and Communications Technology
ISOC	Internal Security Operations Command
LLM	Large Language Model
MHESI	Ministry of Higher Education, Science, Research and Innovation
ML	Machine Learning
NaiST	Natural Language Processing and Intelligent Information System Technology
NLP	Natural Language Processing
NSTDA	National Science and Technology Development Agency
NECTEC	National Electronics and Computer Technology Centre
SPT	Speech and Audio Technology
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organisation
UNDP	United Nations Development Programme
VISTEC	Vidyasirimedhi Institute of Science and Technology Council

Introduction

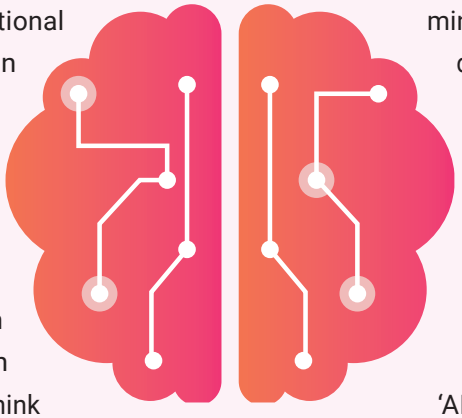
Recent advancements in machine learning have facilitated a surge in transformative advancements in various global sectors including medicine, engineering, and education. This unprecedented progress has led to countries investing heavily in machine learning. The United States and China are at the forefront of these developments, with the competition between the two often being dubbed the 'new space race'[1], a nostalgic reflection of the Cold War era defined by intense military and economic tensions. Just as the space race of the past pitted global superpowers against one other, the digital duel between present-day titans promises a quite similar narrative. It is that the victor of this AI race will steer the course of global technological innovation and societal transformation for the many generations to come.

Beyond global powerhouses, countries such as Thailand are carving their presence in the realm of ML. Despite not being traditionally perceived as a primary player in the arena, Thailand has been making significant strides in its adoption of ML within its principal economic sectors. The Thai government has taken forward-looking steps towards the formulation of an AI policy framework through the National AI Strategy and Action Plan (2022-2027)[2]. This strategic plan has been developed within the broader context of a twenty-year vision that aims to enhance the nation's competitive advantage through collaborations between the public and private sectors while fostering awareness and appreciation for emerging technologies. However, much of Thailand's current discourse on AI remains centred only around infrastructural evolution and data prowess.

In early 2019, The Thai government launched a drive towards formulating the National AI Ethics Guideline[3]. The document lacks enforceability, relying heavily on voluntary adherence instead. Central to the deliberation is the noticeable absence of several stakeholders in drafting the Guideline, especially groups and representatives of the working class—the very people who stand to be most impacted by the economic makeover brought by this tech. This report delves into Thailand's AI readiness viewed through the discerning lens of human rights. This report aims to examine how the country incorporates human rights principles into its AI sectors. We envision that through a rigorous examination, we can identify blind spots and evaluate Thailand's readiness to navigate the rapidly evolving industry without leaving anyone behind.

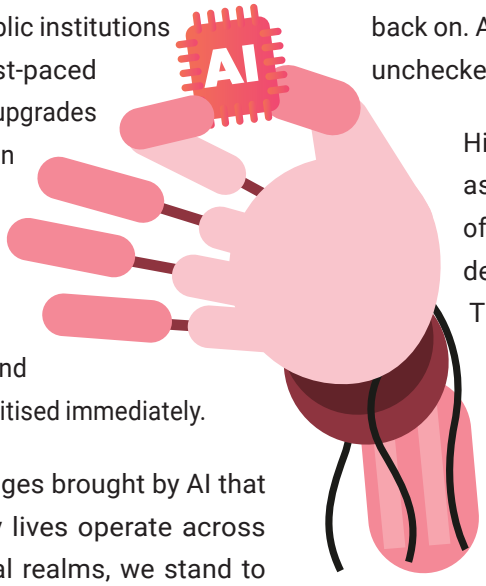
What is machine learning and Artificial Intelligence?

Machine learning and Artificial Intelligence are often used interchangeably but do not mean the same thing. Machine learning is the process of developing algorithms that would allow a computer to learn from data and is capable of assessing additional data to make predictions. On the contrary, no scientific consensus exists on what 'AI' entails[4]. The most used definition is that it focuses on the ability of machines to 'think' and 'communicate' akin to humans[5]. However, worth noting here is how the words think and communicate are enclosed within inverted commas. This is because machines, as non-living organisms, do not possess the consciousness or cognition as humans do. Instead, they emulate these functions based on their programming and the data they have been provided. Despite the recent advancements in LLM, AI has still yet to be achieved. Bearing that explanation in mind, it is appropriate to note that due to prevailing misconceptions and the interchangeable use of ML and AI in various policies, declarations, and other referenced documents, this report will adhere to the original language of the cited text when referring to 'ML' and 'AI' for consistency and clarity.



AI and human rights

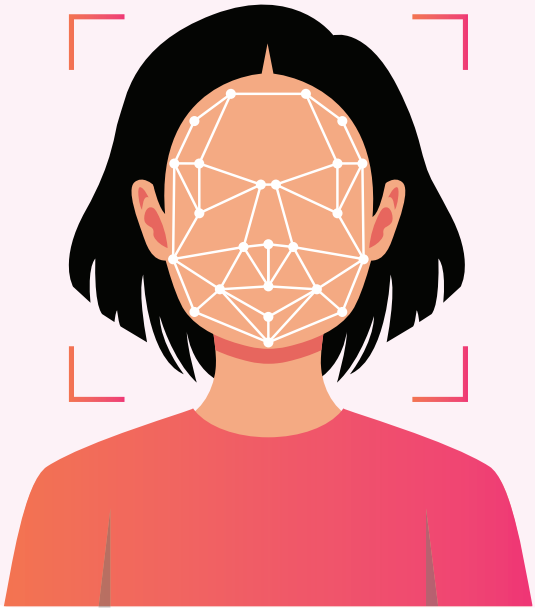
The recent developments in AI technology have highlighted the need to critically assess the preparedness of a government to leverage AI tech effectively and efficiently while respecting human rights. AI technologies, as both dynamic and disruptive[6], pose a big challenge for governments mainly because public institutions are often the last to adapt to such paradigm-shifting innovations. The bureaucratic nature of governmental institutions alongside a long process of procurement and vetting, is often seen as a constraint to rapid technological adoption. The passivity of public institutions stands in contrast to the fast-paced industry of technology, where upgrades and improvements occur within months if not weeks. This, of course, does not mean that regulation should be forestalled. If anything, it calls for tangible actions beyond technical adaptation to be prioritised immediately.



Given the revolutionary changes brought by AI that could impact how our daily lives operate across economic and socio-political realms, we stand to face significant risks should regulatory frameworks be placed at the back seat of the political road maps. Issues including bias, discrimination, and surveillance embedded in machine learning models need to be addressed sooner rather than later to ensure that the benefits outweigh the risks. Tech libertarians, operating within the framework of capitalist self-interest, have argued that self-regulation by developers and investors is enough. For them, regulation stifles innovation. They believe that AI developers are the most qualified to assess the potential and pitfalls of their creations. The core of this belief assumes that corporations have innate benevolence when left alone and that they will always choose the betterment of all over lining the pockets of the few. History tells us otherwise. The Industrial Revolution has shown us how factory owners benefited immensely from the invention of steam power while the workers were subjected to long hours, unsafe work environments and insultingly low wages. This scenario parallels the 'digital sweatshops' of the 21st century, where gig economy workers fuel the need for AI systems to work by performing repetitive tasks such as data labelling. These workers often find themselves at the bottom of the economic pyramid, earning below living wages and lacking social safety nets to fall back on. And this is just one of the examples of what unchecked AI developments look like.

Historically marginalised communities such as aboriginal and indigenous peoples have often been relegated to the periphery of these developments. This is even aggravated by Thailand's non-recognition of indigenous peoples in its Constitution that hinder the rights of indigenous populations to self-determination, as we previously noted in our recent shadow report in 2021[7]. The blatant exclusion of indigenous peoples in official censuses puts them in a more vulnerable situation as they are often reduced to mere 'collateral damages' amidst the so-called march for progress. Another factor worth considering is how AI models need data to thrive. Many corporations have publicly announced their intention to crawl the entire Internet in search of this data. Such data is often extracted from individuals without their explicit consent or compensation. And this is all based on the capitalist belief that since we share content freely, companies have the right to monetise it whenever they want. The data gathered are then used in various ways, including monitoring individuals' online behaviours, identifying popular trends to monetise, and developing targeted advertisements tailored to specific demographic

segments. As usual, the applications of this technology often surpass its initial purpose since governmental authorities employ it for concerning purposes such as surveillance through facial recognition technology.



For instance, we have noted in our recent shadow report with another Thai-based NGO that security officials have randomly collected biometric data including from children of suspected insurgents, such as DNA samples and facial profiles of Malayu Muslims in the Southern Border Provinces (SBPs). Failure to address these apparent problems could result in an unfavourable future that could leave societies and communities woefully ill-prepared to navigate the challenges and opportunities of future technologies. In a country like Thailand, it is important to ensure that technological systems are not used as a political tool to favour corporations and institutions at the expense of the Thai people.

A brief history of AI development in Thailand

The earliest mention of AI in Thailand can be traced back to 1975, when AI was included in a university's curriculum through lecture notes written in the Thai language. In 1992, the Department of Computer Engineering at Kasetsart University founded the inaugural AI laboratory in Thailand[8]. Following that, that same department established the first subdivision of AI research in the country, only dedicated to Natural Language Processing (NLP) known as the Natural Language Processing and Intelligent Information System Technology (NaiST) Lab[9]. Presently, the speciality research unit located at NaiST assumes a leading role in forming and operating the Centre of Excellence for Unified Knowledge and Language Engineering (Uknow-CoE) at Kasetsart University

In 1992, Computer System Consulting Co., Ltd conducted a survey on AI technology in Thailand, which was reported to the country's National Electronics and Computer Technology Center (NECTEC). The survey findings indicated that the areas of focus within the field of artificial intelligence in Thailand were primarily NLP, expert systems, and knowledge engineering. In contrast, comparatively less emphasis has been placed on machine architecture, machine learning, AI software development, and computer vision. Another survey conducted by Kijsirikul and Theeramunkong[10], with the support of the CICC and NECTEC, provided insights into the dynamic progress of AI research and development inside the nation. The 1999 survey identified a noticeable disconnect between public and private interests, resulting in a need for substantial encouragement and incentives for developing more in-depth AI research.

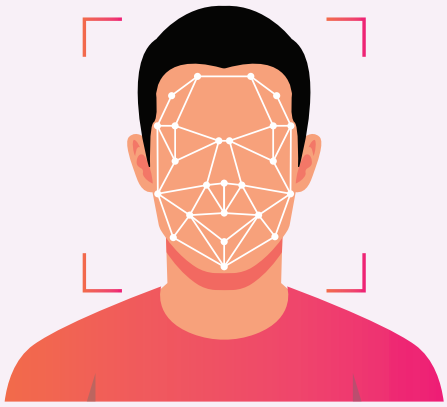
In 2001, Thailand formulated an ICT Master plan to turn the country into a knowledge-based society with five crucial areas of expertise: e-government,

e-education, e-society, e-industry and e-commerce. Between 2006 and 2010, several collaborative initiatives were implemented among research institutes and universities per the national ICT strategy. During this period, the development of AI research in Thailand has focused closely on tangible and assessable impact, such as prototypes and patents, instead of a number of publications alone[11]. By 2010, the development of AI technology in Thailand had witnessed significant growth, encompassing a wide array of subfields from speech processing to robotics. Thailand's focus on applied AI research has positioned the nation within the global AI landscape, particularly in healthcare and agriculture. During this period, a notable project known as Vaja emerged as a pioneer in the field. Vaja was a bilingual Thai-English text-to-speech synthesis developed by the Speech and Audio Technology (SPT) Lab at NECTEC. Vaja has been utilised in over 70 hospitals nationwide as an assistive technology to streamline hospital administrative processes and as an interface for people with visual disabilities to access information online[12].

In 2015, Thailand initiated a series of initiatives to harness the fourth industrial revolution, which the government coined "Thailand 4.0". Thailand 4.0 is an economic model that prioritises innovation and new technology to expand the development of new sectors including robotics, aviation, logistics, biofuels and biochemicals while cementing its role as a regional medical hub[13]. Alongside this development, the Thai government, spearheaded by the Ministry of Industry, also devised a 20-year national strategy that would inform government policies and plans to help achieve the country's goal of becoming a developed country by 2037 by the principles of good governance). In conjunction with the 20-year national strategy, the National Industrial Development Plan was implemented to offer comprehensive directives for advancing provincial, regional, and urban development. One of the earliest manifestations of AI during this period was observed within the police sector. The Government of Thailand initiated an AI system for surveillance and criminal analysis in East Bangkok to prevent petty crimes through facial recognition technology. **Facial recognition technology later expanded in the Deep South provinces of Yala, Pattani and Narathiwat and the districts of Na Thawee, Jana, Tepa and Sabayoi of Songkla.**

According to the government announcement, people who fail to provide facial scans to their service providers AIS, TrueMove H or DTAC will not be able to use their mobile phone services[14] The initiative, primarily undertaken by the Internal Security Operations Command (ISOC), sought to employ facial ID mechanisms for mobile phone users in the provinces above[15]. The Thai military has directed considerable emphasis towards the provinces in the Deep South, where roughly 8,200 surveillance cameras equipped with AI capabilities were deployed in October 2020[16].

South region



In February 2021, the Thai cabinet approved the National AI Ethics Guideline[17], marking a significant milestone in Thailand's history. The guideline aims to provide clarity on the ethical principles that should be adhered to when developing and deploying AI technologies, ensuring alignment with worldwide legal frameworks and standards. In the same year, the Digital Government Development Plan (2020-2022)[18] was approved by the Thailand cabinet to promote collaboration among different sectors, establish well-defined project guidelines, determine budget components, assign responsible agencies, and offer operational guidance to state entities. The establishment of the "Thailand Artificial Intelligence Research Institute" was announced by the Vidyasirimedhi Institute of Science and Technology Council (VISTEC) in partnership with the Digital Economy Promotion Agency (DEPA), with a projected timeline of completion by April 2022[19]. In July of the same year, the cabinet approved Thailand's national AI strategy and Action Plan to develop an effective ecosystem that will encourage the advancement and usage of AI in Thailand. The long-term objective is to stimulate economic growth and improve the overall quality of life for the population. This initiative supports the vision of establishing an efficient ecosystem in Thailand by 2027 that fosters the development and application of AI to enhance both the economy and the well-being of the people. The establishment of the AI Governance Clinic (AIGC) subsequently occurred, seeking to create an exhaustive structure for the regulation of artificial intelligence (AI) in electronic transactions per domestic and international norms and guidelines.

A National Artificial Intelligence Committee meeting, chaired by former Prime Minister General Prayut Chan-o-cha, was assembled in December 2022 to bolster AI development and application[20]. Significant strides in AI governance materialised in the first quarter of 2023. It began with the debut of the AI Governance Guidelines for Executives[21], which was made public on 28 August 2023 through a partnership between Mahidol University and the Electronic Transactions Development Agency (ETDA). In March 2023, IPAP and national/international AI governance experts organised a collaborative discussion on AI Governance in Thailand, focusing on the healthcare sector and AI practices. Following the joint efforts of MHESI and NSTDA in creating the Thailand National AI Strategy and Action Plan 2022-2027, the NSTDA Director announced on 28 August 2023 the "Medical AI Data Sharing" initiative to bolster research and the application of medical AI in the country.

Methodology

In preparing this report, we undertook desk research between August 2023 to January 2024. During this period, our consultant reviewed laws, government publications, news articles and policy documents shaping the growing AI space in Thailand. We used a novel approach to policy assessment by focusing on human rights in the digital space.

The Human Rights-Focused Policy Impact Assessment (HR-PIA) was devised to address the gaps in existing AI readiness frameworks, which predominantly cater to organisations and businesses. Specifically, the HR-PIA aims to close the accountability and liability gaps left by existing AI readiness frameworks. Through a rigorous examination of Thailand's legal policy, this document aims to diverge from traditional PIAs by underlining the strict adherence to human rights norms and policies to ensure that guidelines surrounding emerging technology do not fall prey to empty promises. Further, this methodology employs a set of targeted questions (see Table 1) designed to evaluate the different dimensions of AI policies in Thailand. As such, our methodology shifts away from a rigid and superficial check-the-box approach and instead adopts an HR-PIA that addresses each critical aspect of the technology to ensure that the policies surrounding it prioritise the broader societal implications rather than corporate interests.

Human rights-focused policy impact assessment

Existing frameworks, as put forward by Jolstrom[22] and Horvat & Heimberger[23], have provided valuable insights into measuring a country's readiness for AI adoption. These frameworks, nevertheless, have focused on tangible metrics such as a country's infrastructure, strategic alignment with long-term goals, data capabilities, and workforce skill sets. Sure, there is no denying that these criteria are critical when examining a nation's capacity to harness the potential of AI effectively. It is, however, our observation that these frameworks need to consider the multidimensional impact of AI on society, particularly its ramifications on human rights. Similarly, the UNDP's AI readiness framework and the UNESCO Recommendations on the Ethics of AI have offered standards and principles for using AI ethically. Yet, they have only emphasised the assumption that 'ethical deployment' alone is tantamount to positive human rights outcomes. This perspective is misleading and allows corporations and governments to commit ethics-washing while sidestepping accountability. Since these guidelines are not legally binding, entities risk using them to shield themselves from criticism.

Given this significant gap, our approach involves conducting a detailed human rights policy assessment. The Human Rights-Focused Policy Impact Assessment (HR-PIA) is aimed at (1) evaluating Thailand's legal documents, policies and action plans in relation to AI development in the country and (2) addressing the liability vacuum left by the existing frameworks and guidelines. HR-PIA uses **UNESCO's Readiness Assessment Methodology**[24] as the foundation of the framework but puts **heavier emphasis on human rights assessment** through legal and regulatory, social and cultural, economic, scientific and educational, and technological and infrastructural dimensions. For this, relevant policies and legal documents were analysed to provide an in-depth analysis of Thailand's current AI regulation landscape. By doing so, we seek to foster a more responsible and human rights-centric AI deployment environment that goes beyond non-binding ethical guidelines. Furthermore, this report includes the contributions of two pro-bono law firms, which peer-reviewed and edited sections of the legal analysis of national laws and policies.

The table (see Table 1) below shows the key pattern we must examine when conducting an HR-PIA. The difference between a PIA and an HR-PIA lies in the fact that the latter not only focuses on compliance with international and national human rights norms but also ensures that policies created contribute to the realisation of human rights for all people, especially those who were not involved in the development of the technology. This means that the

primary objective of the HR-PIA is to ensure that working-class people, and not only those who own the means of production, have support and assistance within the system. The questions we laid down in the table below are only guide questions we considered when assessing the legal documents and policy papers we reviewed. Not all questions are expected to be answered.

Table 1 Human Rights-Focused Policy Impact Assessment

Pillar	Assessment Criteria
Policy and governance	
• Impact assessment	Does the policy framework include systematic impact assessments considering the potential human rights implications and harms?
• Regulatory check	Are there established regulations and compliance mechanisms that explicitly enforce human rights standards in AI initiatives?
• Transparency	Are decision-making processes transparent, with active participation from workers and their representatives, and do they align with the principles of open governance and human rights?
Development and operations	
• Inclusive design	Are development processes inclusive, considering the needs and rights of diverse and marginalised groups?
• Bias checks	Are there mechanisms to identify, prevent, and correct biases that may infringe on the right to non-discrimination and equality?
• Privacy protocols	Are privacy protocols in place to ensure the right to privacy and protection from unlawful surveillance and data misuse?
Access	
• Equitable access	Are AI technologies and benefits accessible to all, regardless of socio-economic status, upholding the principle of universal access?
• Stakeholder inclusion	Are all stakeholders, especially marginalised groups, included in the decision-making processes related to AI?
• Awareness drives	Are there initiatives to raise awareness and educate all stakeholders about AI and its implications on human rights?

Pillar	Contextualisation
Oversight	
• Feedback mechanisms	Are there mechanisms for collecting feedback and ensuring the right to remedy and accountability in AI operations?
• Grievance paths without reprisals	Are there clear and secure channels for individuals to raise grievances related to AI without fear of reprisal?
• Audits	Are independent, worker-centric audits conducted to review compliance with human rights standards and norms in AI operations?
Human rights norms	
• Harm prevention	Are AI initiatives designed and implemented with the primary goal of benefiting humanity while preventing potential harm?
• User autonomy	Can people control AI systems that affect them rather than being subjected to unaccountable automated decisions?
• User privacy	Are users' privacy rights respected and protected against unlawful intrusion and data misuse in AI operations?

Thailand’s data protection & privacy rights landscape

Personal Data Protection Act (PDPA) of 2019

Thailand commenced its journey to provide more data protection for individuals (referred to in the Act as 'data subjects') when the PDPA was fully enforced in June 2022. The PDPA is the country's inaugural law that was primarily formulated to govern Thai residents' data protection and data use. The PDPA was drafted with reference to the EU's General Data Protection Regulation (GDPR) and safeguards personal data via restricting collection, usage, disclosure or tampering of data without the owner's informed consent. It has a broad applicability that applies to all organisations, both domestic and foreign, that handle personal data within the jurisdiction of Thailand. Not only is the PDPA enforceable to data activities happening in Thailand, but it also applies to offshore businesses handling Thai residents' data[25]. It is also worth noting that PDPA accounts for the fact that Thai law may not formally recognise some businesses, but it does not discriminate based on this notion alone. In line with international standards, the PDPA has set a legal basis for general data protection, including consent, public interest, withdrawal and rectification[26]. Specifically, data subjects have the following rights under the PDPA:

Right to be informed (Section 23)	The data subject must be informed by the personal data controller, prior to or at the time of the collection of the personal data, of the required details, such as the objective of the collection, the data retention period, and the rights of the data subject, except in cases where the data subject already knows.
Right to access (Section 30)	The data subject can access or request a copy of their data and request information about how the data controller collects, uses, and discloses data.
Right to data portability (Section 31)	The data subject has the right to receive the Personal Data concerning themselves in a format that is readable or commonly used by automatic tools or equipment. It can be used or disclosed by automated means.
Right to rectification (Sections 35 and 36)	The data subject can rectify their incomplete, inaccurate, misleading, or not up-to-date data.
Right to erasure (Section 33)	The data subject can request a data controller to delete or de-identify his/her personal data that the data controller collects, uses, and discloses, except where the data controller is not obligated to do so if the data controller needs to retain such data in order to comply with a legal obligation or to establish, exercise, or defend legal claims.
Right to object (Section 32)	The data subject can object to particular collection, use, and disclosure of his/her data, such as objecting to direct marketing.
Right to restrict the use of data (Section 34)	The data subject can restrict the use of his/her data in certain circumstances.

Right to withdraw consent (Section 33, 2)	The data subject can withdraw his/her consent at any time for the purposes that he/she has consented to the collecting, using, and disclosing of his/her data unless the data subject's right to withdraw his/her consent is restricted by law or by contract which is beneficial to the data subject.
Right to complain (Section 73)	The data subject can complain to the competent authority where he/she believes that the collection, use, and disclosure of his/her data is unlawful or non-compliant with the PDPA.

While the PDPA provides a framework incorporating provisions that implicitly safeguard human rights through its detailed provisions on privacy, the Act does not explicitly mandate impact assessments designed to evaluate potential implications of technologies on human rights. Here, we see how the Act fails to consider potential human rights violations and instead adopts a reactive approach that waits for such violations to occur before taking action. **The PDPA predates the widespread adoption of LLM in mainstream culture. Therefore, the PDPA does not differentiate between automated and non-automated data processing methods. Due to this lack of specificity and broad parameters, the PDPA may unintentionally grant some protections or allowances to businesses which use AI and automation.** Insufficient provisions in the PDPA have resulted in the inability to mitigate illegal data collection through automated means. There have been occasions where it has been acknowledged that the Thai government has breached individuals' privacy through automated data collection. For instance, In 2022, Reuters reported that Thai Minister of Digital Economy and Society, Chaiwut Thanakamanusorn, admitted in parliament that surveillance software is used in cases involving national security or drugs, though he did not specify which agency or individuals were targeted. This admission followed a joint investigation revealing the use of Pegasus spyware on at least 30 government critics, with rights groups accusing Thai authorities of exploiting broad national security definitions to suppress opposition[27].

The privacy standards set in the Act lack specificity when it comes to AI use cases, which means it will not know what to do when confronted with such situations. In Section 19, paragraph 4, PDPA emphasises the concept of consent when it comes to data collection, use and disclosure[28]. However, the phrase "shall utmost take into account that the data subject's consent is freely given" does not provide standards to ensure that consent is freely given. The potential consequence of this situation is the emergence of coercive consent practices, particularly for individuals whose understanding of technology and the law is limited. In this scenario, whether a checkbox automatically signifies consent is a common question. If it does, individuals lacking technical expertise or have a restricted level of literacy may struggle to make well-informed choices about their data. They would probably grant consent to data practices they object to should they better grasp their rights and the consequences of giving consent.

The PDPA has also set limitations on data collection only to the point where it is "necessary in relation to the lawful purpose". This phrase leaves much room for interpretation in a country like Thailand, further complicated by the provisions listed in Section 24 Section 1, which defines these 'lawful purposes,' including the concept of 'public interest.' Under Section 26, the legal obligation to various 'public interests' is enough as a lawful basis to process sensitive personal data without requiring explicit consent from the data subjects. Nevertheless, the precise definition of "public interest" remains pertinent. This loophole could enable the government to collect extensive data on individuals legally using AI technology.

Section 4 of the PDPA has outlined scenarios that would constitute exceptions to safeguards, which raises critical concerns. Under the framework of 'state security,' the government is permitted to collect, use, or disclose personal data without individual consent, which raises concerns about potential impacts on privacy rights and the possibility of politically motivated surveillance. The issue lies not in the exemptions themselves but in the lack of clear guidelines defining the law's scope, leaving these exemptions open to various interpretations. It remains uncertain how, or if, data breaches resulting from government actions will be addressed in the future..

It is worth noting that the PDPA does not explicitly provide systematic impact assessments related to potential human rights violations.

This was even made more evident during the peak of the COVID-19 pandemic when the use of contact-tracing apps raised significant data privacy concerns due to the government's extensive data collection practices. **In January 2021, the Centre for COVID-19 Situation Administration named five Thai provinces as maximum-control zones.** During this time, people living in these provinces were required to use the tracing app, Mor Chana[29]. Failure to comply with the app mandate could lead to penalties, contradicting international privacy standards and affecting those without smartphones. Responding to public frustration, the Prime Minister announced no punishments for not using the app, provided individuals recorded their travel history[30]. Infected individuals would still face charges for concealing information about their visits.

While the PDPA creates structures such as committees to examine complaints and probe into violations, these committees are not designed to evaluate how data protection practices, or the use of AI technology can affect people's human rights. Additionally, the independence of the members of the committee is also worth looking at. To illustrate, the 16-member Personal Data Protection Committee, established in January 2022 to implement the PDPA, primarily consists of government officials as its members[31]. Whether the committee's decisions are independent or subject to any oversight mechanism remains uncertain[31]. In simpler terms, these committees mainly check if the rules of the PDPA are being followed, not necessarily if broader human rights are being protected or violated in the process. Ex-post protection may be afforded to citizens, but it is insufficient as harm has already been committed. Such an approach further necessitates knowledge of the AI's exploitation and the citizen's possession of the necessary resources and understanding to file a claim.

The PDPA builds a robust regulatory framework with well-defined compliance mechanisms to reinforce privacy and data protection standards. The recent

changes in January 2024 illustrate that the committee is willing to adopt the PDPA to the evolving data needs of Thai society. The Expert Committee has just put stronger teeth to the law by making data controllers liable of administrative fines if they neglect to inform data subjects of required information and processing personal data without a legal basis. Despite these changes, concerns have been raised regarding the exemptions the Committee has provided to small businesses. According to the recent changes, small businesses in the manufacturing sector (no more than 200 employees or an annual revenue not exceeding THB 500 million) and in the retail sector (no more than 100 employees or annual revenue not exceeding THB 300 million (approximately USD 8.5 million) are exempted from the obligation to maintain records concerning data processing activities. This is one step forward, two steps back. Businesses and organisations, no matter how big or small they are, must be held liable especially if they are handling customers or members data. This amendment, while framed as a relief for small businesses, does not provide ample protection to the rights of the people they are serving. It further fails to challenge the privately owned data economy and its exploitative practices effectively. Instead, it perpetuates the division within the corporate-digital realm, where we are divided into 'controllers' and 'subjects,' with the latter group lacking empowerment. PDPA is an endorsement of the illusion of freedom while neglecting the power imbalances and economic necessities that compel users to consent to data processing. This brings us to another critical concern: the PDPA's current failure to address access to AI technologies and inclusivity in AI decision-making. The lack of public awareness about data protection rights or AI implications could lead to people not taking their data privacy seriously, potentially leading them to casually consent without understanding its full repercussions.

Cybersecurity Act of 2019

The Cybersecurity Act grants the government broad powers to collect data on Internet users[33].The law empowers the government to access online data and seize the personal devices of individuals when they deem that such data is necessary to ensure the state's stability. In our 2019 study titled *"Thailand's Cybersecurity Act: Towards a human-centred Act. Protecting Online Freedom and Privacy, While Tackling Cyber Threats,"*[34] we identified six key challenges imposed by the Cybersecurity Act:

- Broad scope and definition
- Problematic substantive provisions and failure to define them
- Controversial control mechanisms
- Power play in the application of the Act
- Absence of checks and balances
- Failure to ensure remedies

The Cybersecurity Act is, first and foremost, a law that protects the interest of the state and public order rather than defending individual liberty online. The Act grants the National Cybersecurity Committee wide-ranging powers to guard critical government infrastructure in national security, public health and energy. However, the Act uses a vague definition of "cyberthreat," which might be broadly interpreted to cover any online activity that they feel threatens public order or state security. This lack of clarity is problematic as it grants authorities broad discretion to determine what constitutes a "cyber threat". Without explicit criteria, there is a risk that any online activity, even benign or dissenting, might be classified as a threat if it is perceived to challenge public order or state security in any way. In 2020, 8200 surveillance cameras equipped with AI technologies were deployed in the southern border provinces[35,36] to increase the efficiency of the authorities in "monitoring and

risk notification system" and "ensur[ing] the local population's safety." Here we see how safety, while being the objective, would also lead to heightened surveillance that would appear to control movement of minority communities in the locality.

Similarly, under this existing legal framework, government agencies such as the Anti-Fake News Center have deployed AI technologies to conduct extensive online surveillance, all while lacking transparent public knowledge and discussion, well-defined statutory guidelines, and strong protective measures[37]. In such situations, it is common for individuals to be unaware of attempted or successful intrusions that impinge upon their right to privacy. At the same time, the government may be inclined to exploit this vulnerability. Without explicit safeguards, a transparent system and prior informed consent, the repercussions for privacy and human rights, particularly for vulnerable groups and minorities, have life-threatening implications.

These scenarios also raise some concerns regarding the independence of the National Cybersecurity Committee[38]. Suppose the committee acts under the control of specific political entities or parties, their assessments regarding the definition of a "cyberthreat" are susceptible to bias and lack impartiality. Sections 50 and 51, for instance, grant the Committee broad powers to prescribe characteristics, duties, and responsibilities for organisations involved in maintaining the security of computer systems, with few constraints outlined in the text. This vagueness can result in arbitrary interpretation and application of the law, infringing upon the principle of legitimacy that requires laws to be clear and accessible.

The Cybersecurity Act also does not provide specified safeguards for protecting personal identifiable data. The lack of data security and confidentiality provisions regarding data use and retention threatens privacy rights. Also, according to Sections 73 and 74 of the Cybersecurity Act, private enterprises considered critical information infrastructures to have reporting obligations concerning cybersecurity incidents. Failure to report or submit risk assessment reports could result in imprisonment and heavy penalties. Facebook and Google, for example, reported a handful of government requests to access user data. Google did not comply with any request in 2021 while Facebook provided 65 per cent of the requested data from January to June 2022. While big tech companies can challenge government requirements, this may not be true for small businesses. In October 2019, the Ministry of Digital Economy and Society enforced a data retention provision that requires coffee shops, restaurants, and other venues that offer public Wi-Fi to retain users' data, including names, browsing history and log files, for at least 90 days.

The Cybersecurity Act exemplifies its deficiency in providing independent monitoring mechanisms. When a threat reaches a "crisis" level, it allows searches or seizures without requiring a court warrant and without the possibility of judicial appeal. The lack of accountability provisions for rights violations runs in contrast against the principle of legitimacy that calls for a robust, independent oversight system to authorise relevant surveillance measures. The glaring absence of external oversight over the exercise of governmental powers under this legislation grants officials extensive authority, inevitably paving the way for substantial violations of privacy and autonomy.

Computer Crime Act (CCA) of 2017

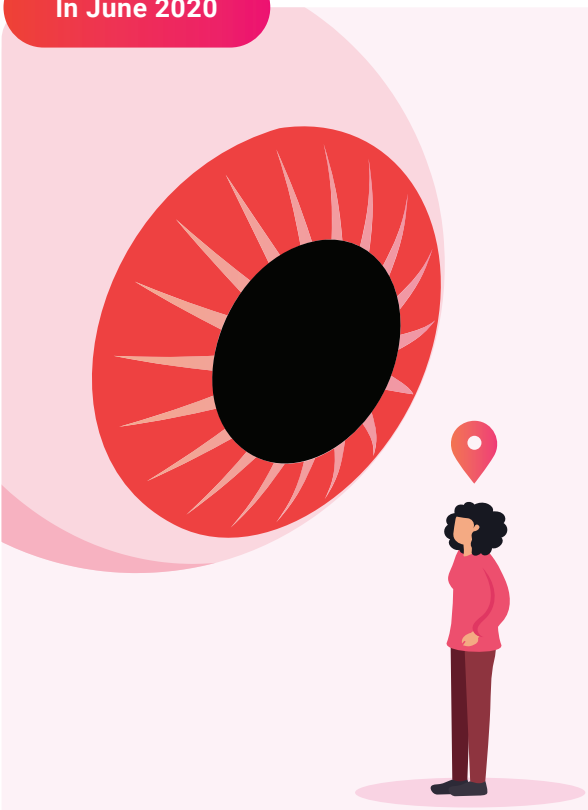
The CCA allows the government to undertake surveillance and warrantless searches of personal information and data. This could undermine the right to use encryption and anonymity, and may force service providers to facilitate surveillance[39]. Under Sections 18 and 19, "competent" officials are the only ones allowed to access and copy computer data, instruct service providers to hand over user data and seize computer systems. While Sections 22-24 penalise the unauthorised disclosure of acquired data, the safeguards against abuse of power by "competent" officials are not robust. In fact, the term "competent" here is noteworthy, as it only signifies that the individual has been appointed to the role, without necessarily implying a high standard of expertise or independence. While the Act does outline qualifications, training, and oversight mechanisms, these measures are limited in ensuring independence from the state. Additionally, there is no established system for public feedback on the enforcement of the CCA, nor are there protections in place for complainants to shield them from potential reprisals.

Section 20 of the CCA allows for the restriction of computer data dissemination if it is deemed to adversely affect national security or contravene "peace, concord, or good morals of the people." However, the vague wording of this provision leaves it open to potential misuse, as it does not clearly define what constitutes a threat to "peace and concord" or a violation of "good morals." This lack of clarity could lead to an overreach of authority, potentially stifling freedom of expression and targeting opposition voices or minority communities, which might result in unjust prosecutions and inhibit free speech. Meanwhile, section 26 further complicates matters by requiring service providers to retain computer traffic data for at least ninety days, and in some cases, up to a year. This mandatory data retention and submission to government authorities raises concerns about infringement on users' privacy rights. Additionally, Section 15 indirectly obliges service providers to monitor user data, as failure to do so or disclose information could be interpreted as tacit approval of activities outlined in Section 14, which includes the dissemination of content that allegedly threatens public security, causes panic, or harms others online.

Additionally, section 20 permits the limitation of computer data dissemination, which could adversely affect national security or contravene the "peace, concord, or good morals of the people." This vaguely phrased provision offers room for exploitation, possibly curtailing freedom of expression since it doesn't precisely define what actions endanger "peace and concord" or violate "good morals." Such lack of clarity raises concerns over potential misuse against opposition voices and minority communities, potentially resulting in unjust prosecutions and inhibiting free speech. Section 26's stipulations further complicate the situation.

Service providers must preserve computer traffic data for at least ninety days, extending to one year. This obligatory data gathering and submission to government bodies infringe on users' rights. Moreover, Section 15 of the CCA indirectly mandates that service providers oversee user data. Failure to monitor or disclose user information could be construed as endorsing activities outlined under Section 14, which encompasses posting content that supposedly undermines public security, induces panic, or inflicts harm on others online.

In June 2020



In June 2020, a confidential document surfaced, disclosing that the Ministry of Defense solicited the National Broadcasting and Telecommunications Commission (NBTC) for mobile location data of individuals diagnosed with COVID-19[39]. This document also outlined a surveillance initiative and a cooperative effort involving major Thai telecom firms and the government to access user data. The provisions in the CCA potentially set the stage for widespread surveillance due to the absence of specificity regarding the type of data to be retained. This lack of detail violates essential principles of necessity and proportionality for any action infringing on privacy rights. The mandated data retention is not adequately aligned with particular legitimate objectives and lacks crucial privacy protections, contravening principles of "necessity and proportionality" and "legitimacy."

National AI Strategy (NAIS)

The Thai government has taken steps towards formulating an AI policy framework through the National AI Strategy and Action Plan (2022-2027). To put the strategy into action, a National AI Committee[41] and sub-committees were formed focusing on the following thematic expertise:(1) Regulation and Social; (2) Data and Infrastructure; (3) Human resources and Research, Development, and Innovation; (4) Industry promotion and Investments[42]. The objective of this action plan is threefold: building human capacity, economic growth, and social and environmental impact. Thailand appears to be on track with this objective as the country has jumped from 60th place in 2020 to 31st in 2022 in the Government AI readiness framework.

On 13 December 2022, the inaugural session of the National Committee was presided over by Prayut Chan-o-Cha, who held the position of Prime Minister during the period. The committee convened to deliberate upon the National AI Strategy[43]. However, as of May 2023, there is a lack of subsequent references to the

National Committee or its endeavours after said date, except for the information available on the website of ETDA. As per the information on the website, it was anticipated that the AI Governance Framework for e-Transaction will be submitted to the committee by June 2023[44]. Yet, the specific responsibilities and outcomes of the committee's input remain unclear today. The same uncertainty applies to the four sub-committees created alongside the National AI Committee. Additional information regarding the development or status of the sub-committees' progress is also currently unavailable[45].

NAIS provides a general framework for AI development in Thailand and appears to bring forward an ambitious goal of making Thailand an AI hub in Southeast Asia. While it includes commendable strategies for infrastructure development and workforce upskilling, it falls short by not addressing and providing specific details on protecting and preserving human rights. The inherent neglect to consider the potential impact of AI technologies on individuals and communities is of notable concern. While the first sub-strategy addresses readiness in law, ethics, and regulations for AI applications, it does not elaborate on how human rights impact assessments will be integrated into the AI development and implementation processes.

Thailand's National AI Strategy and Action Plan (2022-2027) lacks a sufficient articulation of inclusive development processes, which may further perpetuate and exacerbate existing disparities within the society, particularly for diverse and marginalised groups. Biased algorithms, often resulting from biased data or design processes, have life-threatening repercussions should they generate discriminatory results—thereby infringing on individuals' rights to non-discrimination and equality. Aiming for an extensive AI adoption across various public and private agencies while not providing sufficient guidelines and binding legal authorities to monitor these systems amounts to mere posturing. Not only does the plan fail to provide for structures to identify, prevent, and rectify such biases, which is crucial to ensure that AI applications treat all individuals and groups fairly and equitably, it also does not seek to create an environment where the development and the deployment of AI technology would contribute to social equity. And this is even more evident in the glaring omission of ensuring equitable participation and benefit across gender lines. Commitments aimed at increasing the meaningful representation of underrepresented groups in the decision-making process are missing from NAIS. With a significant gap in labour participation rates between men (75%) and women (59%) with women bearing a disproportionate burden of unpaid work, there is a clear and pressing need for policies and strategies that ensure that AI technologies benefit all genders equitably[46]. Another questionable goal within the plan is to increase the number of public and private agencies that use AI technology to a minimum benchmark of 600 agencies in six years. Without explicit reference to the protection of human rights, NAIS inadvertently opens up a Pandora's box of potential human rights violations. The plan has only made it clear that the strategies it laid down would be implemented following the Personal Data Protection Act (PDPA), which, as pointed out in the previous section, lacks adequate safeguards to protect against automated processing of personal data. As a result, NAIS does not bring about any improvements and does not guarantee improved security of private information. Online users remain susceptible to their data being collected through automated collection processes, such as those employed by the Thai government.

The Plan promotes using AI as critical to the country's economic prosperity and human development. And that is all there is to it: an attestation to the country's pursuit of wealth, seemingly relegating human rights to the back seat.

To ensure that these advantages do not overshadow human rights, it is essential to incorporate measures that explicitly establish the connection between AI regulations and human rights. This should be part of the initial thought process and not treated as an afterthought, especially since Thailand has a history of human rights abuses in the digital sphere[47]. Online users are often being charged and prosecuted for merely exercising their freedom of expression, and government agencies have gone as far as using spyware to monitor human rights defenders and activists. Without an adequate framework to prevent excessive and potentially illegal surveillance, the Plan fails to consider the possibility of state-sponsored abuses.

While Thailand's forward-looking National AI Strategy and Action Plan (2022-2027) represents a bold leap towards leveraging AI for national development, it requires substantial revisions to address its shortcomings when it comes to human rights protection, data privacy, inclusivity, accountability, and transparency. A government that is singularly fixated on economic growth is destined to fail in nurturing an equitable society that upholds the rights and dignity of its people. To truly harness the potential of AI in a way that benefits all citizens, not merely the privileged few, the strategy needs to incorporate critical elements that would provide a balanced and responsible framework for AI development and deployment throughout the country.

AI Ethics Guideline

The introduction of the first National AI Ethics Guideline[48] is a commendable step towards fostering responsible AI practices in Thailand. The document initiates a noble endeavour to clarify ethical benchmarks for AI usage, emphasising its commitment to upholding legal standards, international norms, privacy, and human rights. Nonetheless, while the Guidelines are seemingly poised to champion privacy and human rights, a meticulous analysis reveals its toothless nature and non-binding character that could be exploited, particularly in safeguarding human rights.

For example, the Guideline places the responsibility of safeguarding users' rights chiefly on "stakeholders" without stringent mandates. This approach makes the safeguarding of human rights a mere voluntary practice. Thus, it opens the door to further inconsistencies regarding protection measures. The problem here rests on the fallacious assumption that corporations and businesses would prioritise people over profit, a deception that has echoed through the annals of history for far too long. This means that the Guideline has no backbone since it does not translate human rights principles into legal rights and obligations

binding on third parties. Adherence to these 'ethical' guidelines remains at the discretion of corporations. Without a legal imperative to compel compliance, the Guideline risks becoming little more than a comic relief. It naively assumes the sufficiency of the PDPA in guarding human rights despite the flaws we have discussed in previous sections. Another notable deficiency is the inadequate distinction between automated and non-automated data processing by the PDPA.

Furthermore, the Guideline prioritises economic competitiveness above all. It puts the objective of achieving economic stability and viability for the nation at the forefront. This clearly reflects the political and cultural environment in which the Guideline was drafted— a time of significant political upheaval following a coup d'état by the military junta. The economic-centric approach sidelines the critical concerns about citizens' rights and data privacy—leading to a potential compromise for mere economic gains. Additionally, the Guideline grounds itself on Strategy Two of the National 20-Year Strategic Plan, which was exclusively economically driven. The drafting process, conspicuously devoid of civil society and labour groups, inherently reflects an economic-driven agenda, with human rights demoted to a position subordinate to national security. The people are subtly coerced into adapting an AI consciousness instead of being afforded proactive protection against potential AI misuse.

Despite advocating for non-discriminatory practices, the Guideline omits any explicit mention of indigenous peoples, mirroring Thailand's constitutional non-recognition of these groups[49]. This absence of recognition and acknowledgement raises substantial doubts regarding the government's commitment to proactively extend protection from AI-related harms to indigenous and ethnic minority groups within the country. It highlights a significant gap in the Guideline's coverage: it fails to consider and address indigenous peoples' unique challenges and vulnerabilities in the context of AI development. Such a gap can unintentionally sustain inequalities and bias within the technology sector.

Meanwhile, the Guideline has embarked on initiatives to proactively foster women's engagement in the AI sector, strategically addressing the gender gap and promoting robust representation. The Ministry of Digital Economy and Society (MDES) and the National Broadcasting and Telecommunications Commission jointly organised three webinars to commemorate International Girls in ICT Day in 2020. These webinars were designed to prepare them for future employment opportunities in the rapidly evolving labour market. While it is great to see progress towards the inclusion of women in AI development[50], it is also essential to address the remaining shortcomings of the Guideline, especially regarding LGBTIQ+ individuals. For instance, the Guideline does not explicitly address gender beyond the binary, and no considerations were included on how gender bias may affect non-binary people and members of the LGBTIQ+ community. Incorporating a wider spectrum of gender identities and expressions into AI development and policy-making processes is vital to ensure that the technology can mirror and respond to the diversity and complexity of the society it serves.

In the complex legal landscape of Thailand, laws such as the Computer Crime Act[51] and the Cybersecurity Act[52] have provided a cloak for potential invasive practices that enable surveillance and arbitrary searches and seizures under the broad and often nebulous umbrella of "public order" and "national security". When intertwined with the unpredictable algorithms of AI, these laws become potent tools that can be exploited for excessive surveillance and control.

The AI Ethics Guideline certainly acknowledges privacy and security as ethical principles. However, its understanding is rather myopic and insufficient in preventing the potential abuses of AI in infringing upon human rights. Given the intrinsic tendency of AI to perpetuate and amplify existing biases and prejudices within society, the Guideline fails to articulate specific prohibitions against applications of AI that infringe upon international human rights law.

The imperative for effective oversight and redress mechanisms is significant within the capitalist techno-society. Henceforth, it is important to stress that oversight mechanisms should not only be strong and independent but should also serve as protectors of the public's interest against the unchecked power of both the state and the market. In the Guideline, there is an ambiguity regarding which government agencies are tasked with oversight, not to mention the unanswered questions regarding their impartiality, independence, and commitment to protecting privacy and data rights. Specifically, the Guideline mentions oversight by government agencies to prevent unfair competition in producing harmful autonomous weapons and AI technologies. It also states that the government must establish a certification framework for AI to increase the credibility of AI designers, developers, service providers, and their products and services. According to the principles of transparency and accountability, agencies must oversee models and algorithms used by stakeholders to ensure the ability to identify their origins and functions. Additionally, AI development and use are subject to a public reporting mechanism, specifically about their impact on humankind and the environment. These agencies are also responsible for appointing an officer to investigate AI-inflicted harms and working towards their resolution.

When there is an apparent conflict between human rights considerations and the relentless pursuit of competitiveness and profit maximisation, the absence of concrete requirements and liabilities can

be seen as a nod of approval for a technocratic approach to governance and regulation. The Guideline is silent on the intricate relationship between ethics and capital and offers no clear path for navigating these frequently competing imperatives. In the relentless whirlwind of capitalist production, where data has become a new form of capital, the rights of individuals are often sidelined. The Guideline does not provide adequate legal remedies or compensation schemes for individuals adversely affected by AI applications. While the PDPA offers some protections, it is crucial to underline that it does not cover the right to be informed during automated decision-making and profiling processes, which are central to AI technologies. In this era where data is the new oil, the working class finds itself again at the frontline, bearing the brunt of these exploitative practices.

Glaring gaps and insufficiencies remain even if one considers the Guideline in conjunction with other pieces of legislation related to data security and privacy. The Cybersecurity Act, for instance, mandates judicial permission only for specific actions, allowing law enforcement extensive leeway in directly addressing what is perceived as critical threats without the need for judicial oversight. The environment created by the Cybersecurity Act enables authorities to obtain broad investigative powers without requiring judicial authorisation. Thus, it places individual privacy rights on a precarious edge.

The Guideline has adopted a somewhat weak and passive stance concerning the banning of AI applications that violate international human rights laws. It merely encourages government authorities to educate the general public and stakeholders and involve them in the development and responsible use of AI at all stages, considering the potential for prejudice, unfairness, and discrimination. It implies that AI is acceptable as long as it permits human intervention in its operations and decision-making processes, effectively excluding fully autonomous systems. The Guideline also mandates the removal of datasets and algorithms containing inherent bias or unfair elements but places the responsibility on developers to establish an oversight mechanism to ensure the safety of AI systems when complete bias elimination is impossible. In this way, the Guideline primarily serves as a recommendation for corporations and governments to follow when it suits them.

Is Thailand AI-ready?

The short answer is no.

The country's approach to AI proliferation and adoption has been marked with questionable decisions where economic prosperity precedes human rights. Further, significant gaps and loopholes in the country's current judicial framework leave the country unready for responsible AI adoption. Notably, the lack of legally binding mechanisms to criminalise harms brought by excessive use of AI technology has been neglected to pave the way for creating the AI Ethics Guideline. While the Guideline boasts itself as a tool that would ensure that ethics is prioritised in the deployment of AI, it is nothing but a toothless document that corporations and government agencies can use to ethics-wash their use of AI against the public. The departure from a human-centred approach to an economic-centred approach has indeed sidelined the rights of the people for the sake of capital development. With corporations and government agencies left to protect human rights when convenient, the people of Thailand become vulnerable and exposed to exploitation for profit and surveillance. A radical restructuring of the existing framework is imperative to pave the way for human-centred, trustworthy, and responsible AI in Thailand.

Thailand requires a binding law that delineates the rights and obligations of developers, users, governments, and private and public bodies and provides robust safeguards for human rights. This law must be devoid of the exploitative tendencies' characteristic of capitalist structures, ensuring that the benefits of AI are equitably distributed amongst the people rather than accumulating.

We can no longer rely on principle-based approaches alone. Principles fail to mandate explicit obligations or limitations for public institutions, private organisations, or individuals, and offer no enforceable penalties for non-compliance. In saying so, Thailand also needs to go beyond risk-based approaches to regulate AI. In recognising this deficiency, it is imperative that Thailand also transcends the limited scope of risk-based regulation when it comes to AI. Such approaches only focus on mitigating known risks and often fail to address the broader implications of AI on societal norms and human rights. What Thailand needs is a human rights-based approach to AI development, which puts a strong emphasis on human rights throughout the AI system's life cycle. This means ensuring that the interests and human rights of all stakeholders such as creators, end users, developers and those impacted by AI deployments are recognised and upheld. To truly build a human-centred and responsible AI in Thailand, we need to restructure the current framework to commit firmly to human rights principles. This must be in line with international human rights standards related to data protection and privacy rights.

In Table 2, we provide you a summary of various human rights instruments relevant to the right to privacy and freedom of expression alongside Thailand's ratification status of each instrument.

The restructuring of the current AI framework should ensure that domestic laws in the country would maximise the benefits of algorithms for humans and encourage positive collaboration between people and technology. A human rights-based law on AI will establish mandatory rules that guarantee the respect, protection, and promotion of rights, including both economic and socio-political rights. Accordingly, the public should have the opportunity to participate in hearings and consultations during all drafting stages. Since AI should serve humans and not the other way around, technology must be harnessed in a manner

that respects and advances human rights. Any AI law should consider the special needs of vulnerable groups, such as women, individuals in rural areas, queer individuals, and racial and ethnic minorities, as they are more likely to fall victim to harmful algorithmic bias. Concerning data protection, individuals must have the right to be informed about how their data is collected, processed, and stored. After all, a human-centered AI law must consider the people behind the data.

Table 2 Thailand and International Human Rights Treaties (IHRL)

Human rights instruments relevant to Right to Privacy and FOE	Ratification Status
International Convention on the Elimination of All Forms of Racial Discrimination	Ratified/Accession: 2003
International Covenant on Civil and Political Rights	Ratified/Accession: 1996
Optional Protocol to the International Covenant on Civil and Political Rights	Not Ratified/Accession
International Covenant on Economic, Social and Cultural Rights	Ratified/Accession: 1999
Convention on the Elimination of All Forms of Discrimination against Women	Ratified/Accession: 1985
Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women	Signature: 2000, Ratified/Accession: 2000
Convention on the Rights of the Child	Ratified/Accession: 1992
Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict	Ratified/Accession: 2006
Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography	Ratified/Accession: 2006
Optional Protocol to the Convention on the Rights of the Child on a communications procedure	Signature: 2012, Ratified/Accession: 2012
International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families	Not Ratified/Accession
Convention on the Rights of Persons with Disabilities	Signature: 2007, Ratified/Accession: 2008
Optional Protocol to the Convention on the Rights of Persons with Disabilities	Ratified/Accession: 2016

Source: OHCHR, Status of Ratification Interactive Dashboard[53]

A human-centric AI framework in Thailand also necessitates the establishment of strong, independent oversight bodies to protect the public interest against state and market powers. Table 3 illustrates the stance of the Thai government in relation to various global guidelines on Trustworthy AI. A more nuanced explanation on what each guideline represents and endorse can be found on Annex 2.

Table 3 Thailand and Global Guidelines on Trustworthy AI

OECD Recommendation on AI[54]	The first intergovernmental standard on AI; an attempt by the economic collective to promote the use of AI in a responsible and democratic manner. **Thailand has not signed the OECD Recommendation, despite being the only Southeast Asian country to benefit from an OECD Country Program which draws from the four key strategic pillars of good governance and transparency, business climate and competitiveness, "Thailand 4.0" and inclusive growth**[55]**.**
G20 AI Principles[56]	A manifestation of the G20 countries' commitment to create a sustainable and trustworthy AI environment. **The principles have not been endorsed by Thailand.**
UNESCO Recommendation on the Ethics of Artificial Intelligence[57]	The first ever comprehensive global standard-setting instrument to provide AI with a strong ethical basis. Although not legally binding, the Recommendation applies to Thailand by virtue of its membership to UNESCO since 1949. **Thailand adopted the Recommendation,**[58] but no public statements have been made regarding its implementation.
Universal Guidelines for AI[59]	Ethical standards applicable to AI with the goal of ensuring peace, security, and prosperity in their development, as well as the protection of human rights. **These guidelines are endorsed by organisations and individuals, not governments.**

An AI law should stipulate a clear list of prohibited AI systems, grounded in human rights considerations. Thailand can learn significantly from leading entities like the EU, which has banned "unacceptable" uses of AI in sensitive areas, including education, employment, and law enforcement. The EU AI Act, which has recently been made into law at the time of writing this report, established a binding framework for LLMs to ensure that there are no systemic risks present to EU citizens when adopting such technologies. Further, the EU AI Act has also laid down clear and binding obligations for classified systems that are considered as 'high-risk' such as AI systems that have potential harm to health, safety, fundamental rights, environment, rule of law and democracy. EU citizens are also given a right to launch complaints about AI systems and receive explanations about the decisions that the AI system came up with.[60] In Article 5, Section 1(a), it is mentioned that individuals and groups must be protected from harm caused by AI systems that use subliminal or manipulative techniques.This protection is specifically against AI systems that materially distort behavior and impair the ability to make informed decisions, resulting in decisions that cause or are reasonably likely to cause significant harm. The following categories of AI have been deemed by the EU AI Act as high-risk and, therefore, requires high quality data, documentation and traceability, transparency, human oversight, accuracy and robustness to mitigate the risks to fundamental rights and safety:

In a move that is unpopular among private industry, the European Commission has implemented a substantial revenue-based fine mechanism to address non-compliant developers. This means, according to Article 101 of the Act, that providers of general-purpose AI models can be fined up to 3% of their total worldwide annual turnover in the preceding financial year. Additionally, the European Parliament issued a resolution in 2020 urging Member States to "establish a common strict liability regime for high-risk autonomous AI systems" and to apply "a risk-based approach that might encompass several levels of risk, based on clear criteria and an appropriate definition of high risk."[61] But the issue with risk-based approach is that it inherently positions corporate interests as potentially equal to, or even more important than,

fundamental human rights. This leads us to a scenario wherein the very protection of these rights could be compromised in order to build the technology. The Act also does not adequately address the power of major tech companies, which is the root of all the problems. Driven by neoliberalism and constant desire for profit, BigTech firms have significant influence over the development and deployment of AI technologies. Legislation is no longer sufficient to prevent these companies from leveraging AI to increase their dominance in the market, potentially entrenching their power even further.

On 17th of May 2024, the Council of Europe adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law[62] after two years of drafting. This document boasts itself as the first binding treaty on AI, focusing on protecting human rights, democracy and the rule of law, and it will be open for States' signature from 5 September 2024. Thailand, for instance, could enhance its existing regulations by considering the convention's guidelines outlined in Chapter 5, which advocate for principles like transparency, accountability, and non-discrimination. These guidelines promote the development of AI technologies that are both ethically sound and socially beneficial, emphasising measures that are meant to protect human rights, democracy, and the rule of law. This approach will allow for the adoption of globally informed but locally tailored strategies that respect Thailand's unique social context.

In saying so, the convention is not without its criticisms. One major concern is the leeway it provides to states under the banner of sovereignty, allowing them the discretion to implement or disregard moratoriums on certain AI practices. This flexibility, while respecting national autonomy, could potentially lead to a regulatory "race to the bottom," where nations compete to attract business through lenient AI regulations, possibly compromising worker rights and safety standards in the process. The exclusion of national defense from the convention's scope is troubling. Such exclusions open the door to less regulated, possibly opaque AI activities in sensitive areas such as national defence, raising fears about inadequate oversight and transparency in practices that could have significant ethical and societal implications. Thailand can leverage these gaps to forge a path that addresses the broader data governance issues omitted by the Framework Convention. The convention's lack of focus on data monopolies, cross-border data flows, and the economic exploitation of data by BigTech firms presents a critical area where Thailand could innovate. By incorporating strict regulations and oversight measures that specifically target these areas, Thailand can protect against the potential regulatory capture that might favour corporate interests over public good. This would involve crafting policies that ensure fair competition, protect personal and non-personal data, and maintain transparency in AI practices.

Building on the pivotal resolution[63] (A/78/L.49) adopted by the UN General Assembly in March 2024, Thailand stands to gain significant insights and guidance on navigating the challenges and opportunities presented by AI. This landmark document not only addresses the pressing need for ethical guidelines in AI development but also underscores the critical balance between technological advancement and human rights protection, particularly the right to liberty, security, and justice. For instance, the resolution explicitly addresses the potential threats posed by the malicious design and misuse of AI technologies. Clause three of the resolution identifies risks that include the undermining of sustainable development and the violation of fundamental human rights. For Thailand, this is a crucial area of focus as the nation seeks to integrate AI in various sectors such as law enforcement, public health, and education. Ensuring that AI systems are designed with safeguards against misuse is essential to prevent them from becoming tools of discrimination or oppression. To promote equitable access to AI benefits, Thailand should implement policies with teeth that address

the needs of its diverse population. This includes tailoring AI solutions to the local context and ensuring they are accessible to individuals across different economic, social, and geographical backgrounds.

The UN Commissioner for Human Rights, who has advocated for a worldwide ban on dangerous AI, also underscores the importance of transparency and accountability in applying AI to meet real-life needs[64]. These practices should adequately guide Thailand in formulating its own approach to legislating technology, ensuring that accountability gaps at all stages of production and development chains are effectively addressed. Clear legal remedies and compensation for those harmed by AI should also be established, safeguarding the rights of the working class from profit-driven exploitation. This initiative can be led by a mechanism that conducts due diligence and provides independent oversight to monitor AI systems. An oversight body should also have the authority to issue opinions and interpretive guidance on law implementation, and to address the impact of AI systems on human rights, rule of law, and inclusive societies.

While enacting an AI law in Thailand that regulates AI and guarantees human rights protection is ideal, practical challenges abound. The government's endeavours to enhance the nation's economic status—evidenced by initiatives like 'Thailand 4.0' and the National AI Strategy—position AI as key to realising these economic goals. However, there is a noticeable tendency to prioritise economic aims over potential human rights concerns arising from AI use. This approach, along with a general lack of public awareness about the risks of unregulated AI, suggests that balancing the benefits and challenges of AI is not viewed as an immediate or crucial issue. Given this context, it is improbable that an AI law effectively safeguarding human rights will be enacted soon. Although the National AI Strategy is set to run until 2027, there is no specified timeline for introducing AI legislation. A truly human rights-based AI policy would emphasise the necessity for AI to operate under frameworks that are not just adaptable and international, but explicitly designed to redistribute power and resources more equally among the global community, especially benefiting those in developing nations like Thailand. The focus on leveraging existing international frameworks could be seen as a call to challenge the hegemonic control of AI technologies by capitalist BigTech entities and instead advocate for a governance model that supports state-led initiatives and public ownership of AI infrastructure.

As Thailand ventures further into the digital future, it is not only advisable but essential to establish a human-centred AI framework. **As is shown in Table 4, Thailand's AI Guideline fails in almost every aspect of what an ethical AI standard should look like. This is even more embarrassing when compared to various international standards such as the UNESCO Recommendation and the EU AI Act.** This framework would be a start to ensure that the potential of AI as a tool for social good is divided to all, so it does not risk becoming another instrument of capitalist exploitation and control. With a human-centred AI framework, Thailand can genuinely harness the transformative power of AI, fostering a digital landscape where technology serves the people, not the other way around.

Table 4 Is the Thailand AI Guideline in alignment with some global AI governance standards?

Ethical and Legal Aspects of AI	The Guideline	The UNESCO Recommendation[65]	The EU AI Act[66]	Council of Europe's Framework Convention on AI[67]
Binding or non-binding nature of the instruments and enforceability of rules	✗	✗	✓	✓
Non-human-centered v. human-centered approach	✗	✓	✓	✓
Discriminatory bias and unfair use mitigation	✓ ✗ some shortcomings	✓	✓	✓ *Article 10 explicitly mentions equality within the life cycle of AI systems.
Gender bias considerations	✓ ✗ no consideration of non-binary people and the LGBTIQ+ community	✓ ✗ no consideration of non-binary people and the LGBTIQ+ community	✓ *Article 5, Section 1(g) mentions mentions LGBTIQ+ people in the context of biometric categorisation systems	✓ *Only the words 'gender equality' was mentioned.
Adequate data protection guarantees in the context of AI use	✗	✓	✓	✓
Prohibited AI uses	✗	✓	✓ *Article 5, Section 1(h) places strict regulations on the use of live facial recognition technology.	✓ *Article 16 calls for the need for a moratorium or ban on certain uses.
AI oversight and ethical governance	✓ oversight by government agencies ✗ lack of clarity	✓	✓	✓
Legal remedies and compensation scheme for victims of AI harm	✗	✓	✓	✓

Recommendations

To promote a human rights-centric, trustworthy, and responsible AI landscape in Thailand, the following recommendations are proposed for various key stakeholders, as outlined based on the preceding analysis. Four primary actors were identified who hold key functions in enhancing the state of data protection and privacy rights in Thailand and ensuring that AI is used to advance human rights.

First, the **Government of Thailand** has a responsibility to uphold and protect the right to privacy and other rights related to AI, such as non-discrimination, human dignity, and fairness, in accordance with international human rights standards. It also plays a critical role in fostering a responsible and human rights-based AI ecosystem. Second, **Members of Parliament** act as intermediaries through which the government can fulfil its responsibilities. Their crucial role extends beyond the mere formulation of laws and regulations; they are accountable for ensuring the effective implementation of legislation that aligns with existing standards. Third, **businesses**, particularly those involved in AI development and data collection, have a responsibility to respect human rights and address any abuses. They play a significant role in shaping the AI landscape and should prioritise human-rights based and responsible AI practices. Finally, **civil society groups** are instrumental in representing the needs of the people and safeguarding privacy rights. Their advocacy, expertise, and efforts contribute to a more privacy-respecting and human rights-based AI landscape, ensuring that individuals' rights are protected as AI technologies continue to evolve.

The Thai Government has several crucial obligations to fulfil:

- safeguard the human right to privacy, aligning with the international human rights law enshrined in Article 12 of the UDHR and Article 17 of the ICCPR. Any state interference in privacy should be confronted fiercely unless it is demonstrably essential, proportionate, and in pursuit of legitimate, class-conscious objectives.
- undertake comprehensive reviews and amendments to current laws, policies, and regulations pertinent to AI, such as the CCA, Cybersecurity Act, PDPA, and National Intelligence Act. This process is crucial for addressing and rectifying broad provisions, violations of human rights, unchecked powers, and the absence of accountability and transparency, thus ensuring alignment with international human rights standards.
- amend the PDPA to eliminate loopholes that exempt data collection under the guise of "national security" as currently permitted in Section 4. The state must adhere to strict legal and evidentiary standards in its use of AI, automation, and biometrics, with a focus staunchly placed on safeguarding human rights and ensuring due process.
- integrate enforcement mechanisms for international digital rights and human rights principles into the 2023-2026 National Action Plan on Business and Human Rights. These mechanisms, grounded in best practices, should guide the development, deployment, and utilisation of AI as a key priority area.
- develop and implement safeguards against the potential abuse of AI surveillance technologies by the State. This development requires establishing effective and independent oversight mechanisms to curb unfettered executive discretion, offering redress mechanisms for victims of surveillance-related abuses.
- engage in public consultations and human rights and algorithmic impact assessments

prior to the procurement and during the deployment of AI systems. Extensive public consultations should involve civil society, human rights groups, and representatives of marginalised or underrepresented end-users.

- impose restrictions on governmental data collection and enforce measures for accountability. Businesses should similarly be mandated to undergo impact assessments and audits of AI technologies while establishing external accountability mechanisms. It is essential to implement laws with real teeth—robust, enforceable regulations that not only impose strict restrictions on governmental data collection but also require businesses to rigorously assess and audit their AI systems.

- prevent any coercive collaboration with tech companies, ISPs, and telecom providers in state surveillance efforts. This includes a prohibition of the use of mandates or any undue pressure that compels these companies to participate in the monitoring or collecting of data on citizens without their explicit consent.

- encourage and fund the development of decentralised AI technologies that empower communities rather than centralise power. This can include supporting open-source projects and community-based AI initiatives that are transparent and accountable to the users they serve.

- promote public investment on open datasets that are representative while respecting privacy and data protection. Such an initiative supports an environment conducive to unbiased AI research and development and improves interoperability and the use of standards.

- require AI systems to be designed with environmental considerations in mind, promoting energy-efficient algorithms and the responsible use of resources to mitigate the ecological impact of large-scale AI infrastructures.

- commit to policies and mechanisms that actively promote women and LGBTIQ+ rights through AI. There must also be a commitment involving consultations with indigenous communities and minority groups during the AI system's design and development stages to minimise bias and privacy breaches.

- mandate that businesses disclose how their algorithms might perpetuate social, cultural, and economic inequalities. Alongside this, the policies should reflect Thailand's diverse population in AI development teams and training datasets, promoting equal access to AI technologies and their benefits for all, particularly marginalised groups and Indigenous peoples.

Members of the Parliament should initiate the following crucial activities:

- advocate for amendments to existing legislation, including the CCA, Cybersecurity Act, PDPA, and National Intelligence Act within the National Legislative Assembly (NLA). Such amendments should address current shortcomings, aligning with international human rights standards as delineated in the UDHR and ICCPR. MPs should also secure consensus among colleagues to guarantee the incorporation of these amendments into the respective Acts.
- introduce a robust whistleblower protection for workers who expose unethical AI practices. These protections would shield whistleblowers from retaliation, provide them with legal and financial support, and ensure that their disclosures lead to genuine change rather than being swept under the corporate rug.
- introduce and support legally binding instruments that seamlessly convert the AI Ethics Guideline into complex, obligatory laws that are binding for all AI stakeholders, including private sector enterprises and government agencies that are involved in the development, deployment, and utilisation of AI systems.
- propose a bill on algorithmic accountability, aiming to eradicate algorithmic discrimination (based on gender, sexual orientation, race, religion, and disability) in both the public and private sectors. This bill should include provisions for significant penalties, such as punitive damages and mandatory public disclosures for organisations found in violation. It should also introduce penalties for individuals who willfully engage in or authorise discriminatory AI practices.
- establish a consistent mechanism for government accountability through a review board. This board should have the authority to impose sanctions, halt AI projects, and demand revisions to AI systems that pose risks to individual rights. The board should be tasked with ensuring that all governmental AI initiatives are transparent, equitable, and free from discrimination.

Businesses are urged to

- reframe business goals to prioritise the interests of a broader group of stakeholders, including employees, communities, and environment, rather than focusing solely on maximising shareholder value. This model will help promote a human rights-based approach to AI development that considers its social, economic, and environmental impacts.
- shift from shareholder-driven models to cooperative or employee-owned structures where profits are shared among all workers and decisions are made democratically. This approach fosters a sense of ownership and accountability among all members and ensures that the benefits of AI are distributed more equitably.
- reinforce to all personnel, particularly those involved in the AI life cycle (engineers, developers, data technicians) that operations should be guided by human rights responsibilities.
- update all company policies and terms of service to reflect a commitment to human rights. This involves transparent communication about the use of AI technologies and automation, detailing how user data is collected, stored, and shared.
- implement robust safeguards ensuring that the design, deployment, and implementation phases of AI are compliant with human rights standards.
- actively reduce the adverse effects on human rights and vigorously pursue adherence to the following principles: ISO 26000, the Toronto Declaration, the Global Network Initiative (GNI), and the Charter of Human Rights and Principles for the Internet. When national laws or regulations conflict with international standards, it is crucial to prioritise these global benchmarks to maintain the highest ethical standards in human rights.
- ensure that their AI strategies and operations are aligned with the UN Guiding Principles on Business and Human Rights despite its non-binding status. This involves conducting thorough human rights due diligence processes to identify, prevent, mitigate, and account for how they address their impacts on human rights.
- ensure that company policies, as well as terms of service, are human-rights centred. There should be clear communication to the public on the usage of AI technologies and automated techniques, including the methods of user data collection, storage, and sharing.

Civil society should

- establish a people's oversight council for AI composed of representatives from various working-class communities in Thailand including labour unions, and marginalised groups. Its primary role would be to monitor AI deployments and intervene in cases where these technologies perpetuate class disparities or infringe on human rights.
- spearhead educational initiatives that not only raise awareness about the technical aspects of AI and data rights but also educate the public on the socio-economic impacts of AI under capitalist frameworks. These campaigns should aim to mobilise public opinion towards a transformation of AI development and us that prioritise communal benefits over private profits.
- enhance the involvement of women, LGBTIQ+ individuals, and other marginalised groups in AI by supporting their participation in AI policy and development spaces. This may include creating inclusive tech spaces, and promoting policies that favour open-source AI solutions. The aim is to democratise AI knowledge and tools, making them accessible to all, thereby reducing the technological hegemony of for-profit enterprises.
- act as a formidable force in national AI discussions to advocate for governance frameworks that dismantle monopolistic AI power structures and promote equitable distribution of AI benefits.
- persistently support vulnerable groups by advocating for AI systems that are designed to reduce labor exploitation and enhance worker rights. This includes campaigning against AI used for invasive surveillance and labour management practices that exploit workers, and promoting AI that assists in labour organisation and rights enforcement.
- be cautious in forming partnerships with technology companies, particularly those known for exploiting AI for profit maximisation at the expense of public interest. CSOs should establish clear ethical guidelines and criteria for collaboration to ensure that any engagement with tech companies aligns with human rights principles and community empowerment. If there is substantial evidence that a partnership would primarily serve the interests of the tech company rather than the public or could lead to misuse or exploitation of the developed technologies, civil society should refrain from collaboration. This stance helps safeguard the integrity of civil society initiatives and promotes the development of AI that genuinely serves the people.

Bibliography

- Bangkok Post. "Committee Finalised for Data Protection Act." January 20, 2022. https://www.bangkokpost.com/business/2250263/committee-finalised-for-data-protection-act.
- Baxter, Will. "Thailand 4.0 and the Future of Work in the Kingdom." March 29, 2017. https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/meetingdocument/wcms_549062.pdf.
- Brackenbury, Ian, and Yael Ravin. "Machine Learning and the Turing Test." 2002. https://ieeexplore.ieee.org/document/5386870.
- Center for AI and Digital Policy. "Universal Guidelines For AI." https://www.caidp.org/universal-guidelines-for-ai/. See also: The Public Voice. "Universal Guidelines for Artificial Intelligence." October 23, 2018. https://thepublicvoice.org/ai-universal-guidelines/.
- CNA. "Data Privacy Concerns Over Thailand's COVID-19 Contact Tracing App Amid New Wave of Cases." February 8, 2021. https://www.channelnewsasia.com/news/asia/transparency-thailand-covid19-contact-tracing-app-mor-chana-14096014.
- Computer Crime Act B.E. 2560 (2017). 2017. http://web.krisdika.go.th/data//document/ext809/809777_0001.pdf.
- Cybersecurity Act, B.E. 2562 (2019). 2019. https://cyrilla.org/en/entity/4nywjpircms?file=1588770279351q8g2xeaybw.pdf&page=1.
- Davenport, Thomas. "From Analytics to Artificial Intelligence." Journal of Cultural Analytics, October 15, 2018. https://www.tandfonline.com/doi/full/10.1080/2573234X.2018.1543535.
- DGA. "The Digital Government Development Plan Of Thailand (English version)." February 11, 2022. https://www.dga.or.th/wp-content/uploads/2022/02/Presentation-DGA-TRANSLATED-INTO-ENG-Vfinal.pdf.
- European Parliament. "Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI." 2023. https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.
- European Parliament. "Artificial Intelligence Liability Directive." 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.
- ETDA. "AI Governance Guideline 2023." https://www.etda.or.th/th/pr-news/AI-Governance-Gui.aspx.
- Freedom House. "Freedom on the Net 2022: Thailand." 2022. https://freedomhouse.org/country/thailand/freedom-net/2022.
- Global Network Initiatives. "GNI Principles." https://globalnetworkinitiative.org/gni-principles/.
- Heimberger, Heidi, Djerdj Horvat, and Frank Schultmann. "Assessing AI-Readiness in Production—A Conceptual Approach." 2023. https://link.springer.com/chapter/10.1007/978-3-031-18641-7_24.
- Holmström, Jonny. "From AI to Digital Transformation: The AI Readiness Framework." 2022. https://www.sciencedirect.com/science/article/pii/S0007681321000744.
- Ian Brackenbury & Yael Ravin. "Machine Learning and the Turing Test." 2002. https://ieeexplore.ieee.org/document/5386870.
- Kawtrakul, Asanee, and Prasong Praneetpolgrang. "A History of AI Research and Development in Thailand: Three Periods, Three Directions." AI Magazine, 2014. https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/2522/2430.
- Kijsirikul, Boonserm, and Thanaruk Theeramunkong. "Survey on Artificial Intelligence Technology in Thailand." Final report, 1999. http://107.167.189.191/~boonserm/publication/AISurvey.pdf.

- Kirsh, David. "Foundations of AI: The Big Issues." October 1990. https://adrenaline.ucsd.edu/kirsh/Articles/BigIssues/big-issues.pdf.
- Manushya Foundation. "Thailand's Cybersecurity Act: Towards a Human-Centred Act Protecting Online Freedom and Privacy, While Tackling Cyber Threats." 2019. https://www.manushyafoundation.org/study-on-cybersecurity-act.
- Manushya Foundation. "Thailand UPR III 2021 - Factsheet: Indigenous Peoples' Rights in Thailand." September 9, 2021. https://www.manushyafoundation.org/thailand-third-upr-cycle-factsheet-indigenous-peoples-rights.
- Manushya Foundation, JPF, Thai CSOs Coalition for the UPR, Thai Business & Human Rights Network. "Joint Civil Society Report on the Implementation of the ICERD (Replies to the List of Themes CERD/C/THA/Q/4-8), for the Review of the Combined Fourth to Eight Periodic Reports of Thailand (CERD/C/THA/Q/4-8) at the 105th Session of the Committee on the Elimination of Racial Discrimination." November 15 - December 3, 2021. https://www.manushyafoundation.org/_files/ugd/a0db76_214b6e0d18594a72b9ad3878a1785bfc.pdf.
- Manushya Foundation, Access Now, Article 19, and the ASEAN Regional Coalition to #StopDigitalDictatorship. "Digital Rights in Thailand: Joint Submission to the UN Universal Periodic Review (UPR) for Thailand's Third UPR Cycle, 39th Session of the UPR Working Group." March 25, 2021. https://www.manushyafoundation.org/digital-rights-joint-upr-submission.
- Manushya Foundation, and Freedom House. "Freedom of the Net Thailand's Country Report, 2022 Edition." 2022. https://freedomhouse.org/country/thailand/freedom-net/2022.
- National Electronics and Computer Technology Center (NECTEC). "The Cabinet Approved the (Draft) Thailand National AI Strategy and Action Plan (2022 – 2027)." July 30, 2022. https://www.nectec.or.th/en/about/news/cabinet-national-ai-strategy.html.
- Nation Thailand. "Bangkok Police to Pilot AI Surveillance System." July 25, 2019. https://www.nationthailand.com/in-focus/30373672.
- NSTDA. "Prime Minister Chairs the First Meeting of National AI Committee." December 13, 2022. https://www.nstda.or.th/en/news/news-years-2022/prime-minister-chairs-the-first-meeting-of-national-ai-committee.html.
- OHCHR. "Artificial Intelligence Risks to Privacy Demand Urgent Action – Bachelet." 2021. https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet.
- Open Development Mekong. "Digital Thailand – AI Ethics Guideline." 2021. https://data.opendevelopmentmekong.net/library_record/digital-thailand-ai-ethics-guideline.
- Personal Data Protection Act, B.E 2562. 2019. https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf.
- Prachatai English. "Citizen Journalists on Police Watchlist." July 14, 2022. https://prachatai.com/english/node/9910.
- Royal Thai Government Gazette. "Annulment of Emergency Situation Announcement in All Areas of Thailand." September 29, 2022. https://ratchakitcha.soc.go.th/documents/139D232S0000000004700.pdf.
- UNESCO. "Readiness Assessment Methodology: A Tool of the Recommendation on the Ethics of Artificial Intelligence." Document code: SHS/REI/BIO/REC-AIETHICS-TOOL/2023, 2023. https://doi.org/10.54678/YHAA4429.
- World Economic Forum. "Forget the Space Race, the AI Race Is Just Beginning." May 8, 2018. https://www.weforum.org/agenda/2018/05/ai-is-the-new-space-race.

Endnotes

1. World Economic Forum, "Forget the space race, the AI race is just beginning," May 8, 2018, https://www.weforum.org/agenda/2018/05/ai-is-the-new-space-race.

2. National Electronics and Computer Technology Center (NECTEC), "The Cabinet approved the (Draft) Thailand National AI Strategy and Action Plan (2022 – 2027)," July 30, 2022, https://www.nectec.or.th/en/about/news/cabinet-national-ai-strategy.html.

3. Open Development Mekong, "Digital Thailand – AI Ethics Guideline," 2021, https://data.opendevelopmentmekong.net/library_record/digital-thailand-ai-ethics-guideline.

4. David Kirsh, "Foundations of AI: The Big Issues," October 1990, https://adrenaline.ucsd.edu/kirsh/Articles/BigIssues/big-issues.pdf.

5. Ian Brackenbury and Yael Ravin, "Machine Learning and the Turing Test," 2002, https://ieeexplore.ieee.org/document/5386870.

6. Thomas Davenport, "From Analytics to Artificial Intelligence," Journal of Cultural Analytics, October 15, 2018, https://www.tandfonline.com/doi/full/10.1080/2573234X.2018.1543535.

7. Manushya Foundation, JPF, Thai CSOs Coalition for the UPR, Thai Business & Human Rights Network, "Joint Civil Society Report on the Implementation of the ICERD (Replies to the List of Themes CERD/C/THA/Q/4-8) for the Review of the Combined Fourth to Eight Periodic Reports of Thailand at the 105th session of the Committee on the Elimination of Racial Discrimination," November 15 - December 3, 2021, https://www.manushyafoundation.org/_files/ugd/a0db76_214b6e0d18594a72b9ad3878a1785bfc.pdf.

8. Asanee Kawtrakul and Prasong Praneetpolgrang, "A History of AI Research and Development in Thailand: Three Periods, Three Directions," AI Magazine, 2014, https://ojs.aaai.org/index.php/aimagazine/article/view/2522/2430.

9. Ibid.

10. Boonserm Kijsirikul and Thanaruk Theeramunkong, "Survey on Artificial Intelligence Technology in Thailand," final report, 1999, http://107.167.189.191/~boonserm/publication/AISurvey.pdf.

11. Asanee Kawtrakul and Prasong Praneetpolgrang, "A History of AI Research and Development in Thailand: Three Periods, Three Directions," AI Magazine, 2014, https://ojs.aaai.org/index.php/aimagazine/article/view/2522/2430.

12. Elina Noor and Mark Manantan, "Raising Standards Data and Artificial Intelligence in Southeast Asia," 2022, https://asiasociety.org/sites/default/files/inline-files/ASPI_RaisingStandards_report_fin_web_0.pdf.

13. Will Baxter, "Thailand 4.0 and the Future of Work in the Kingdom," March 29, 2017, https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/meetingdocument/wcms_549062.pdf.

14. Manushya Foundation and Freedom House, "Freedom of the Net: Thailand's Country Reports," 2020, https://freedomhouse.org/country/thailand/freedom-net/2020.

15. Nation Thailand, "Bangkok Police to Pilot AI Surveillance System," July 25, 2019, https://www.nationthailand.com/in-focus/30373672.

16. Manushya Foundation and Freedom House, "Freedom of the Net: Thailand's Country Reports," 2023, https://freedomhouse.org/country/thailand/freedom-net/2023.

17. Open Development Mekong, "Digital Thailand – AI Ethics Guideline," 2021, https://data.opendevelopmentmekong.net/library_record/digital-thailand-ai-ethics-guideline.

18. Digital Government Agency (DGA), "The Digital Government Development Plan of Thailand," February 11, 2022, https://www.dga.or.th/wp-content/uploads/2022/02/Presentation-DGA-TRANSLATED-INTO-ENG-Vfinal.pdf.

19. The Nation Thailand, "New Research Centre Aims to Offer Readymade AI Solutions to All Sectors," April 2022, https://www.nationthailand.com/pr-news/business/40014357.

20. NSTDA, "Prime Minister chairs the first meeting of National AI Committee," December 13, 2022, https://www.nstda.or.th/en/news/news-years-2022/prime-minister-chairs-the-first-meeting-of-national-ai-committee.html.

21. Electronic Transactions Development Agency (ETDA), "AI Governance Guideline 2023," https://www.etda.or.th/th/pr-news/AI-Governance-Gui.aspx.

22. Jonny Holmström, "From AI to digital transformation: The AI readiness framework," 2022, https://www.sciencedirect.com/science/article/pii/S0007681321000744.

23. Heidi Heimberger, Djerdj Horvat, and Frank Schultmann, "Assessing AI-Readiness in Production—A Conceptual Approach," 2023, https://link.springer.com/chapter/10.1007/978-3-031-18641-7_24.

24. UNESCO, "Readiness assessment methodology: a tool of the Recommendation on the Ethics of Artificial Intelligence," Document code: SHS/REI/BIO/REC-AIETHICS-TOOL/2023, 2023, https://doi.org/10.54678/YHAA4429.

25. Manushya Foundation & Partners, "Digital Rights in Thailand, UPR Submission to inform Thailand's UPR III," March 2021, https://www.manushyafoundation.org/_files/ugd/a0db76_d54eaee422fc41d393153e218422a0d0.pdf.

26. Personal Data Protection Act, B.E. 2562 (2019)," Unofficial translation, https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf.

27. Reuters, "Thailand admits to using phone spyware, cites national security", 25 October 2024, https://www.reuters.com/world/asia-pacific/thailand-admits-using-phone-spyware-cites-national-security-2022-07-20/

28. "Personal Data Protection Act, B.E. 2562," 2019, https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf.

29. Channel News Asia, "Data Privacy Concerns Over Thailand's COVID-19 Contact Tracing App Amid New Wave of Cases," February 8, 2021, https://www.channelnewsasia.com/news/asia/transparency-thailand-covid19-contact-tracing-app-mor-chana-14096014.

30. Royal Thai Government Gazette, "Annulment of Emergency Situation Announcement in All Areas of Thailand," September 29, 2022, https://ratchakitcha.soc.go.th/documents/139D232S0000000004700.pdf.

31. Bangkok Post, "Committee Finalised for Data Protection Act," January 20, 2022, https://www.bangkokpost.com/business/2250263/committee-finalised-for-data-protection-act.

32. Manushya Foundation and Freedom House, "Freedom of the Net Thailand's Country Report, 2022 Edition," 2022, https://freedomhouse.org/country/thailand/freedom-net/2022.

33. "Cybersecurity Act, B.E. 2562," May 27, 2019, https://cyrilla.org/en/entity/4nywjpircms?file=1588770279351q8g2xeaybw.pdf.

34. Manushya Foundation, "Thailand's Cybersecurity Act: Towards a Human-Centred Act Protecting Online Freedom and Privacy, While Tackling Cyber Threats," 2019, https://www.manushyafoundation.org/study-on-cybersecurity-act.

35. Asia Sentinel, "Thai Military Strategy in the Deep South: Surveillance State," June 1, 2020, https://www.asiasentinel.com/p/thai-military-strategy-in-the-deep

36. New Mandala, "The Patani Panopticon: Biometrics in Thailand's Deep South," May 27, 2020, https://www.newmandala.org/the-patani-panopticon-biometrics-in-thailands-deep-south/.

37. Prachatai English, "Citizen Journalists on Police Watchlist," July 14, 2022, https://prachatai.com/english/node/9910.

38. Manushya Foundation, Access Now, Article 19, and the ASEAN Regional Coalition to #StopDigitalDictatorship, "Digital Rights in Thailand: Joint Submission to the UN Universal Periodic Review (UPR) for Thailand's Third UPR Cycle, 39th Session of the UPR Working Group," March 25, 2021, https://www.manushyafoundation.org/digital-rights-joint-upr-submission.

39. "Computer Crime Act, B.E. 2560," 2017, http://web.krisdika.go.th/data//document/ext809/809777_0001.pdf.

40. Thai Enquirer, "Thai Coronavirus Response Center is Sharing Mobile Tracking Data with the Ministry of Defense," June 9, 2020, https://www.thaienquirer.com/14139/thai-coronavirus-response-center-is-sharing-mobile-tracking-data-with-the-ministry-of-defense/; Bangkok Post, "Govt Denies Phone Tracking," June 9, 2020, https://www.bangkokpost.com/thailand/general/1931432/govt-denies-phone-tracking.

41. NSTDA, "Prime Minister Chairs the First Meeting of National AI Committee," December 13, 2022, https://www.nstda.or.th/en/news/news-years-2022/prime-minister-chairs-the-first-meeting-of-national-ai-committee.htm.

42. Asia Society Policy Institute, "Thailand, Artificial Intelligence," https://asiasociety.org/policy-institute/raising-standards-data-ai-southeast-asia/ai/thailand.

43. OECD.AI, "Thailand's AI Strategy to Boost Economic and Social Wellbeing," August 15, 2022, https://oecd.ai/en/wonk/thailand-ai-strategies

44. ETDA, "AI Governance Clinic," https://www.etda.or.th/th/Our-Service/AIGC/index.aspx.

45. OECD.AI, "Thailand's AI Strategy to Boost Economic and Social Wellbeing," August 15, 2022, https://oecd.ai/en/wonk/thailand-ai-strategies

46. The World Bank, "Thailand Gender and Inclusion Knowledge Management Notes," March 8, 2023, https://www.worldbank.org/en/country/thailand/brief/thailand-gender-and-inclusion-knowledge-management-notes.

47. Freedom House, "Freedom on the Net 2022: Thailand," 2022, https://freedomhouse.org/country/thailand/freedom-net/2022; Manushya Foundation, "Digital Rights in Thailand: Thailand's Third Universal Periodic Review Cycle," September 9, 2021, https://www.manushyafoundation.org/thailand-third-upr-cycle-factsheet-digital-rights.

48. Open Development Mekong, "Digital Thailand – AI Ethics Guideline," 2021, https://data.opendevelopmentmekong.net/library_record/digital-thailand-ai-ethics-guideline.

49. Manushya Foundation, "Thailand UPR III 2021 - Factsheet: Indigenous Peoples' Rights in Thailand," September 9, 2021, https://www.manushyafoundation.org/thailand-third-upr-cycle-factsheet-indigenous-peoples-rights

50. UNESCO, "Girls in ICT Day Thailand - Webinars on Artificial Intelligence (AI)," 2020, https://events.unesco.org/event?id=1221714180&lang=1033; ITU, "Girls in ICT Day Celebration, Thailand," https://www.itu.int/net4/ITU-D/CDS/gq/GICT2020/display.asp?ProjectID=1374.

51. "Computer Crime Act B.E. 2560 (2017)," 2017, http://web.krisdika.go.th/data//document/ext809/809777_0001.pdf.

52. "Cybersecurity Act, B.E. 2562 (2019)," 2019, https://cyrilla.org/en/entity/4nywjpircms?-file=1588770279351q8g2xeaybw.pdf&page=1.

53. OHCHR, "Status of Ratification Interactive Dashboard," https://indicators.ohchr.org/.

54. OECD Legal Instruments, "Recommendation of the Council on Artificial Intelligence, Adherents," https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#adherents.

55. OECD, "A Solid Partnership Between Thailand and the OECD," https://www.oecd.org/southeast-asia/countries/thailand/; OECD, "The OECD and Thailand," November 2019, https://www.oecd.org/southeast-asia/countries/thailand/Brochure_ThailandCP-2019.pdf.

56. MOFA Japan, "G20 AI Principles," https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_08.pdf.

57. UNESCO, "Recommendation on the Ethics of Artificial Intelligence," https://en.unesco.org/artificial-intelligence/ethics.

58. UNESCO, "UNESCO Member States Adopt the First Ever Global Agreement on the Ethics of Artificial Intelligence," November 25, 2021, last update April 20, 2023, https://www.unesco.org/en/articles/unesco-member-states-adopt-first-ever-global-agreement-ethics-artificial-intelligence.

59. Center for AI and Digital Policy, "Universal Guidelines For AI," https://www.caidp.org/universal-guidelines-for-ai/. See also: The Public Voice, "Universal Guidelines for Artificial Intelligence," October 23, 2018, https://thepublicvoice.org/ai-universal-guidelines/.

60. European Parliament, “Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI,” 2023, https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.

61. European Parliament, “Artificial Intelligence Liability Directive,” 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf.

62. Council of Europe. 133rd Session of the Committee of Ministers. Strasbourg, 17 May 2024. “Committee on Artificial Intelligence (CAI): Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.” Accessed July 22, 2024. https://rm.coe.int/1680afae3c.

63. United Nations General Assembly, ““Seizing the opportunities of safe, secure, and trustworthy artificial intelligence systems for sustainable development”, 2024, https://www.undocs.org/Home/Mobile?FinalSymbol=A%2F78%2FL.49&Language=E&DeviceType=Desktop&LangRequested=False

64. OHCHR, “Artificial Intelligence Risks to Privacy Demand Urgent Action – Bachelet,” 2021, https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet.

65. UNESCO. Recommendation on the Ethics of Artificial Intelligence. SHS/BIO/PI/2021/1. 2022. 43 pages: illustrations. Also available in Français, Español, Português, 汉语, العربية, Lietuvių kalba, монгол хэл. CC BY-NC-SA.

66. European Union. Artificial Intelligence Act. OJ L, 2024/1689, 12 July 2024. Came into force 1 August 2024. Originally published 13 March 2024. Commission proposal 2021/206. Council vote 21 May 2024.

67. Council of Europe. 133rd Session of the Committee of Ministers. Strasbourg, 17 May 2024. “Committee on Artificial Intelligence (CAI): Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.” Accessed July 22, 2024. www.coe.int/cm.

Annex 1

Global Guidelines on Trustworthy AI

Universal Guidelines for AI	Ethical standards applicable to AI with the goal of ensuring peace, security, and prosperity in their development, as well as the protection of human rights.
OECD Recommendation on AI	The first intergovernmental standard on AI; an attempt by the economic collective to promote the use of AI in a responsible and democratic manner. The principles have not been endorsed by Thailand.
G20 AI Principles	A manifestation of the G20 countries' commitment to create a sustainable and trustworthy AI environment.
UNESCO Recommendation on the Ethics of Artificial Intelligence	The first ever comprehensive global standard-setting instrument to provide AI with a strong ethical basis. Thailand adopted it.

UNESCO Recommendation on the Ethics of Artificial Intelligence

At the international level, UNESCO adopted the first ever comprehensive global standard-setting instrument to provide AI with a strong ethical basis, on November 24, 2021. The UNESCO Recommendation on the Ethics of Artificial Intelligence (the "Recommendation") sets a normative framework and entrusts states with the responsibility of applying it at the national level. This Recommendation enshrines not only a set of values and principles, but also concrete policy recommendations for their practical realization, and provides guidance on how states and stakeholders can address the ethics of AI. The ethical guiding compass seeks to ensure that the emerging technologies serve humanity as a whole and are developed in people's best interests. The Recommendation lays out four values and ten principles to be respected by all actors involved in the AI system life cycle in order to ensure that innovation and development are not hampered, and that international human rights and fundamental freedoms are upheld.

Acknowledging the impacts that AI may have on human lives, the first value enshrined is the "respect, protection and promotion of human rights and fundamental freedoms and human dignity" throughout the life cycle of AI systems. The second one stresses that the "environment and ecosystem flourishing" shall be recognised, protected, and promoted through the life cycle of AI systems. Furthermore, it highlights the necessity to "ensure diversity and inclusiveness" throughout the life cycle of AI systems, consistent with international law, including human rights law. Last but not least, the Recommendation calls on AI actors to play a participatory and enabling role to ensure the "living in peaceful, just, and interconnected societies," which should be promoted throughout the

AI system's life cycle in order to avoid jeopardizing human safety or dividing and turning people against one another.

To facilitate their understanding and operationalization in policy statements and actions, the above-mentioned values are expanded upon in more developed principles, as follows: (1) proportionality and "do no harm"; (2) safety and security; (3) fairness and non-discrimination; (4) sustainability; (5) right to privacy and data protection; (6) human oversight and determination; (7) transparency and explainability; (8) responsibility and accountability; (9) awareness and literacy; (10) multi-stakeholder and adaptive governance and collaboration.

The Recommendation stresses, among others, that AI actors have to promote social justice and non-discrimination, in compliance with international law, and highlights the necessity to take actions to minimise discriminatory or biased applications. Further, privacy is recognised as an essential right to protect human dignity and autonomy, and the Recommendation calls for "[the] data for AI systems [to] be collected, used, shared, archived, and deleted in ways that are consistent with international law and in line with the values and principles set forth in this Recommendation." Additionally, the Recommendation contends that data protection frameworks and governance mechanisms need to be established in a multi-stakeholder approach, safeguarded by the judiciary. Recognised as an essential pillar for the ethical use of AI systems, final human determination is encouraged to be applied for irreversible or difficult to reverse decisions, while life and death decisions must not be entrusted to AI systems. Also, certain uses of AI systems are prohibited, such as

OECD Recommendation on AI and G20 AI Principles

Adopted in May 2019, the OECD Recommendation constitutes an attempt by the economic collective to promote the use of AI in a responsible and democratic manner, in line with its other policy activities on AI dating back to 2016. It was developed by a team comprising 50 experts from various disciplines and sectors. OECD had previously released a series of papers on AI, including the Framework or Classification of the AI Systems, AI definition and life cycle, and Artificial Intelligence in Society. Given their nature, it is left to the OECD member and non-member states to implement the Recommendation in advancing the "stewardship of trustworthy AI." As of May 2023, a total of 46 governments–38 OECD members and 8 non-members–have adhered to the Recommendation.

The OECD Recommendation is the first intergovernmental "ethics code" composed to harness the proliferation of AI and it echoes standards contained in other international instruments, such as the use of AI to drive inclusive growth, sustainable development, and well-being; the incorporation of human-centered and democratic values, fairness, diversity, and human intervention safeguards in operating AI; transparency and explainability of AI systems to ensure users' understanding of AI-based outcomes and how to challenge them; robustness, security and safety by means of continuous assessments and management mechanisms; and accountability of organisations and individuals partaking in the development, deployment, or operation of AI technologies.

Governments are prescribed recommendations on how to implement the above principles. They are expected to facilitate public and private investment in research and development which drive AI innovations. Further, AI ecosystems must be supported with sufficient digital infrastructure, technologies, and mechanisms which allow data and knowledge sharing. Implementation must be done by ensuring a policy environment which accommodates the deployment of trustworthy AI systems and empowering individuals with AI skills and, crucially, uphold a fair transition for workers whose livelihood may be affected by this technology in the interest of the labour market.

Finally, the OECD Recommendation highlights cross-border and cross-sector cooperation to "progress on responsible stewardship of trustworthy AI."

The OECD appoints the Committee on Digital Economy Policy (CDEP), the same body charged with formulating the draft proposal for the Recommendation and convening an expert panel, to follow-up on and monitor the implementation of the Recommendation. The CDEP carries out this role by means of the OECD Policy Observatory, a cutting-edge digital hub created to provide data and AI policies from over 60 countries, and to help stakeholder groups, businesses, and partners communicate findings and conduct evidence-based policy AI analyses.

Foreseeing the importance of applying ethics principles to AI technology, in June 2019, the G20 Digital Ministers drew upon the OECD Recommendation and adopted the G20 AI Principles. The Principles are a manifestation of the G20 countries' commitment to create a sustainable and trustworthy AI environment through inclusivity, human-centricity, transparency, robustness, and accountability. The G20 is an international forum, comprising 19 countries and the European Union, representing the world's major developed and emerging economies. The G20 countries, through a Ministerial Statement, stressed that AI use must be tailored to achieve improvements in the work environment and quality of life, and to create "opportunities for everyone, including women and girls as well as vulnerable groups." G20 countries further recognised the importance of continuing the promotion of privacy rights and personal data security in this context.

Universal Guidelines for AI

The Universal Guidelines for AI were initiated by Professor Marc Rotenberg, President of the Electronic Privacy Information Centre (EPIC) and released in Brussels on October 23, 2018. The Guidelines were one of the first to outline ethical standards applicable to AI with the goal of ensuring peace, security, and prosperity in their development, serving as the prototype for subsequent instruments on the same. In its Explanatory Note, it is mentioned that the Guidelines should be "adopted in national law and international agreements and built into the design of systems." The Guidelines adopt some of the earlier AI ethics instruments and privacy legislation in force at the time, including the Council of Europe Convention 108 (The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), the GDPR (the regulation in EU law on data protection and privacy in the European Union and the European Economic Area), Japanese AI R&D Guidelines (AI research and development guidelines that significantly influenced global AI policies), and the US Privacy Act of 1974 (a federal law that governs the collection and use of records that is maintained in system of records by federal agencies).

According to the Guidelines, there are 12 primary responsibilities pertaining to AI systems: (1) transparency; (2) human determination; (3) identification obligation (that the institution responsible for an AI system must be publicised); (4) fairness; (5) assessment and accountability obligation; (6) accuracy, reliability, and validity obligations; (7) data quality obligation (i.e. data provenance, quality assurance and relevance of input data); (8) public safety obligation; (9) cybersecurity obligation; (10) prohibition of secret profiling; (11) prohibition on unitary scoring (otherwise known as the "social scoring" system); and (12) termination obligation (when human control of the system is no longer possible).

Annex 2

International human rights law in relation to AI

Right to privacy	
ICCPR	**Article 17(1):** No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
UDHR	**Article 12:** No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
Non-discrimination	
ICCPR	**Article 2(1):** Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognised in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. **Article 3:** The States Parties to the present Covenant undertake to ensure the equal right of men and women to the enjoyment of all civil and political rights set forth in the present Covenant.
UDHR	**Article 2:** Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.
Accountability and redress mechanisms for violations	
ICCPR	**Article 2(3)(a):** [Each State Party to the present Covenant undertakes:] [t]o ensure that any person whose rights or freedoms as herein recognised are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; **Article 2(3)(b):** To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy. **Article 2(3)(c):** To ensure that the competent authorities shall enforce such remedies when granted.
UDHR	**Article 8:** Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted [to] him by the constitution or by law.
Right to liberty, security, and justice	
ICCPR	**Article 9(1):** Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law.
UDHR	**Article 3:** Everyone has the right to life, liberty and security of person.

Freedom of expression, to hold opinions, and to receive and impart information	
ICCPR	**Article 19(1):** Everyone shall have the right to hold opinions without interference. **Article 19(2):** Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
UDHR	**Article 19:** Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.
Freedom of association and peaceful assembly	
ICCPR	**Article 21:** The right of peaceful assembly shall be recognised. No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order, the protection of public health or morals or the protection of the rights and freedoms of others. **Article 22(1):** Everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests.
UDHR	**Article 20(1):** Everyone has the right to freedom of peaceful assembly and association.

Right to privacy: Aside from the ICCPR and UDHR, other international and regional human rights instruments contain similar provisions that recognise the importance of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice. The international standards also call for states to respect and protect the right to privacy in the digital age. A report of the UN Special Rapporteur on the right to privacy also clarifies the ethical and legal basis for the processing of personal data by an AI system. It provides that the legitimate usage of AI solutions must meet the following requirements:

1. the law must be drafted in line with "democratic principles and human rights," address "the conflict of interests between managers and the data subjects" and provide "appropriate safeguards for the protection of data subject rights";

2. AI can be applied when it is needed "for the fulfillment of a contract with the data subject and has their explicit consent." The data subject should be given free, uninfluenced consent on an informed basis, and the opportunity to object to the processing within a reasonable time period.

3. AI solutions must be "bound by and limited to the purpose for which it was originally designed, implemented, and correctly documented." The report also identifies a list of rights of individuals whose personal information or identifiable personal information are processed by AI to safeguard the privacy and data security, including the right to understand and query, to withdraw consent, to object to the data processing and the right to erasure and purge the data, among others.

Non-discrimination: The principles of non-discrimination and equality are embedded within both the ICCPR and UDHR. In the context of AI, these principles are relevant given the risks of bias which may arise from AI algorithms and AI-facilitated decision-making. Indeed, the potential of AI to exacerbate existing inequalities within society is one of the main reasons for AI regulation and ethical standardisation Minority or marginalized groups are

especially prone to this AI-based discrimination and must therefore be afforded enhanced protection by means of sufficient transparency, auditability, and accountability in AI design, development, and deployment.

Accountability and redress mechanisms for violations: The degree of autonomy embedded in AI systems render accountability a challenging area to tackle. In addition, AI systems frequently operate on complex software and machineries, making it difficult to predict the potential harm caused by their outputs and take mitigating steps. As such, present regulatory frameworks and ethics guidelines place much emphasis on human intervention as well as transparency in AI deployment. Such an intervention is needed even where an AI can make decisions independently based on machine learning or other techniques. This is to allow the attribution of responsibility to natural or legal persons, which may encompass developers, designers, government entities, and companies. Under international human rights law, accountability should entail prompt and adequate reparations, either through judicial or nonAnnex 1.

Right to privacy: Aside from the ICCPR and UDHR, other international and regional human rights instruments contain similar provisions that recognise the importance of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice. The international standards also call for states to respect and protect the right to privacy in the digital age. A report of the UN Special Rapporteur on the right to privacy also clarifies the ethical and legal basis for the processing of personal data by an AI system. It provides that the legitimate usage of AI solutions must meet the following requirements:

4. the law must be drafted in line with "democratic principles and human rights," address "the conflict of interests between managers and the data subjects" and provide "appropriate safeguards for the protection of data subject rights";
5. AI can be applied when it is needed "for the fulfillment of a contract with the data subject and has their explicit consent." The data subject should be given free, uninfluenced consent on an informed basis, and the opportunity to object to the processing within a reasonable time period.
6. AI solutions must be "bound by and limited to the purpose for which it was originally designed, implemented, and correctly documented." The report also identifies a list of rights of individuals whose personal information or identifiable personal information are processed by AI to safeguard the privacy and data security, including the right to understand and query, to withdraw consent, to object to the data processing and the right to erasure and purge the data, among others.

Non-discrimination: The principles of non-discrimination and equality are embedded within both the ICCPR and UDHR. In the context of AI, these principles are relevant given the risks of bias which may arise from AI algorithms and AI-facilitated decision-making. Indeed, the potential of AI to exacerbate existing inequalities within society is one of the main reasons for AI regulation and ethical standardisation. Minority or marginalized groups are especially prone to this AI-based discrimination and must therefore be afforded enhanced protection by means of sufficient transparency, auditability, and accountability in AI design, development, and deployment.

Accountability and redress mechanisms for vio- judicial avenues. Transparency is an important aspect as it allows defendants access to information which may assist them in making their case against AI-facilitated human rights abuses.

Right to liberty, security, and justice: In many countries, AI technology has grown increasingly prevalent in the field of criminal justice and law enforcement. Improper use of or disproportionate reliance on AI to detect suspicious activities, identify suspects, assist judges

in sentencing or determining bail or parole terms, or forecasting crime rates, may give rise to human rights implications. International human rights law dictates that every individual enjoys protection from arbitrary arrest and detention, fair trial guarantees, and security of their person. This translates into AI developers' and states' obligation to minimise, to the best extent possible, harmful biases, as succinctly clarified by the OHCHR:

For systems whose use presents risks for human rights when deployed in certain contexts, States will need to regulate their use and sale to prevent and mitigate adverse human rights impacts both within and outside the State's territory."

Freedom of expression, to hold opinions, and to receive and impart information: Governments and companies use data collected through AI technology to moderate content publicised by individuals online, directly impacting people's freedom to express their opinions and disrupting the free flow of information. These rights, according to international human rights law, may only be narrowly limited, without compromise. Limitations must be provided by law, carried out with a legitimate aim, and consistent with the necessity and proportionality metrics. While there is a scarcity of authoritative instruments which clarify how these standards apply to AI systems, the accepted understanding is that countries bear the responsibility not to create an environment which facilitates the proliferation of AI to silence free expression. Countries must therefore refrain from imposing any duty upon companies or other entities to filter or block content on their platforms on arbitrary grounds. They often do so by providing incentives for such companies to restrict information or otherwise levying sanctions for failure to do so or compelling the surveillance of users and the handover of their data to government agencies, everything without users' consent and the establishment of an independent oversight body to carry out human rights impact assessments.

Freedom of association and peaceful assembly: The contemporary understanding of right to assembly and association includes the right to use social media and create posts, joining online discussion threads, writing comments on news websites, and others. As such, AI use which limits or in any way impacts these activities would fall within the scope of international human rights discourse. The UN Human Rights Council, for instance, has noted its concern with regard to "undue restrictions preventing Internet users from having access to or disseminating information at key political moments, with an impact on the ability to organise and conduct assemblies." In another resolution, it also noted "that although an assembly has generally been understood as a physical gathering of people, human rights protections, including for the rights to freedom of peaceful assembly, of expression and of association, may apply to analogous interactions taking place online." This fortifies the idea that states carry the responsibility to ensure that people can exercise such freedoms in the digital space, including through guarantees of protection from violence, discrimination, harassment, or other forms of abuse.

MANUSHYA
#WeAreManushyan ∞ Equal Human Beings

Copyright