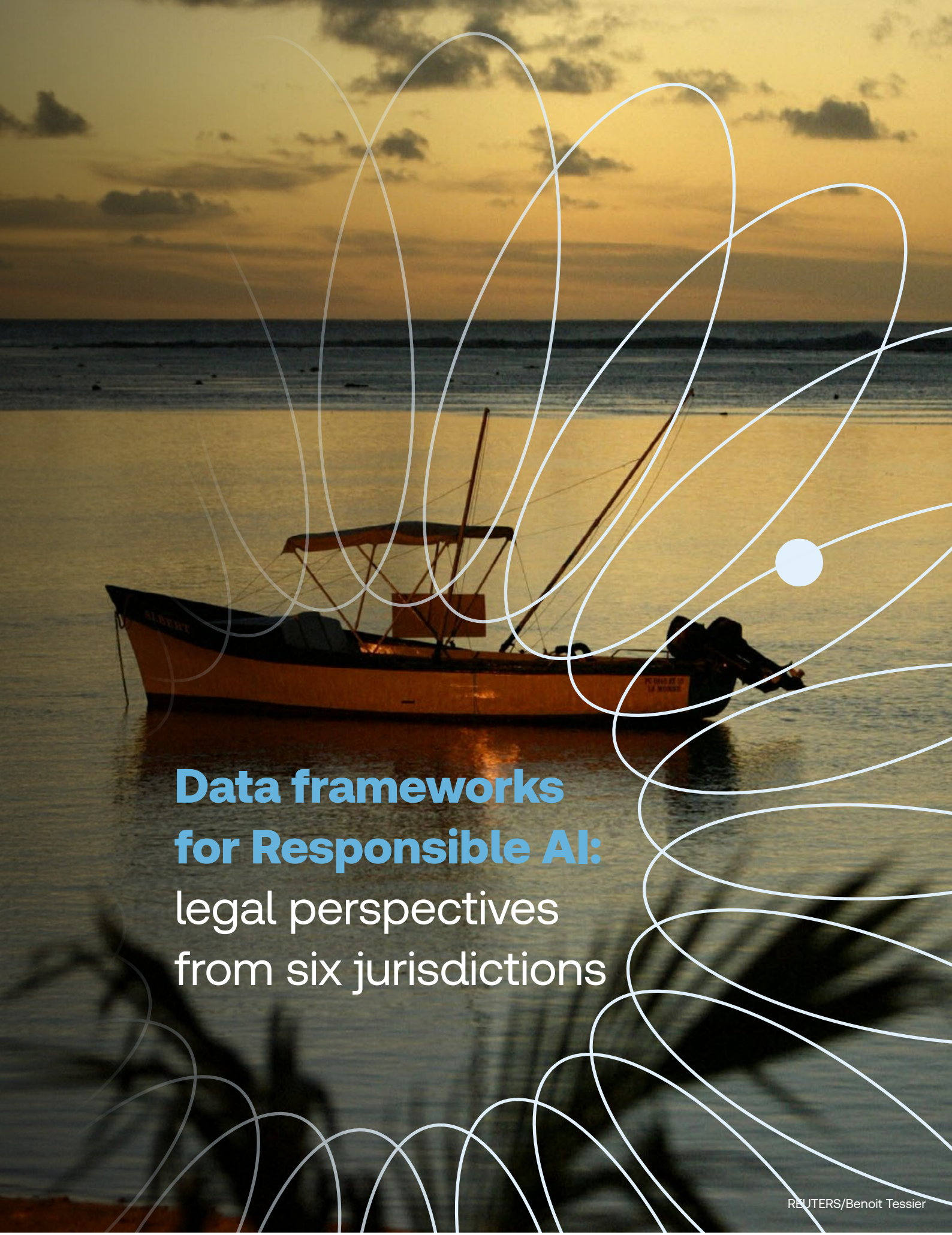

Data frameworks for Responsible AI: legal perspectives from six jurisdictions

REUTERS/Benoit Tessier

TrustLaw | Thomson Reuters Foundation

ODC open data charter

Patrick J McGovern FOUNDATION

Acknowledgements

We are grateful to the law firms that have participated in this research on a pro bono basis through the connection facilitated by TrustLaw, the global legal pro bono network of the Thomson Reuters Foundation, through a partnership with the Patrick J. McGovern Foundation: Basham Ringe & Correa S.C. in Mexico; ObradorDigital SpA in Chile; Prof. Albert Mumma & Company Advocate in Kenya; SyCip Salazar Hernandez & Gatmaitan in the Philippines; Bowmans in Mauritius; and Lee and Li, Attorneys-at-Law in Taiwan.

Disclaimer of liability

This report is offered for information purposes only. It is not legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances. We intend the report's contents to be correct and up to date at the time of publication, but we do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. Open Data Charter; Civic House; Basham Ringe & Correa S.C.; ObradorDigital SpA; Prof. Albert Mumma & Company Advocate; SyCip Salazar Hernandez & Gatmaitan; Bowmans; and Lee and Li, Attorneys-at-Law, the Thomson Reuters Foundation, and the Patrick J. McGovern 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.

The law firms mentioned above generously provided pro bono research to Open Data Charter, through Civic House. However, the contents of this report should not be taken to reflect the views of the law firms or the lawyers who contributed.

Similarly, Thomson Reuters Foundation is proud to support our TrustLaw member Civic House, and its resident organization Open Data Charter, with their work on this report, including with publication and the pro bono connection that made the legal research possible. However, in accordance with the Thomson Reuters Trust Principles of independence and freedom from bias, we do not take a position on the contents of, or views expressed in, this report.

About Open Data Charter

The Open Data Charter is a collaboration between over 200 governments and organizations working to open up data based on a shared set of principles. The six ODC principles were developed in 2015 by governments, civil society, and experts around the world to represent a globally-agreed set of aspirational norms for how to publish data. We are a global civil society organization that promotes policies and practices that enable governments and CSOs to collect, share, and use well-governed data, to respond effectively and accountably to the following areas of work: anti-corruption, climate action, gender, artificial intelligence and data rights.

About TrustLaw (Thomson Reuters Foundation)

The Thomson Reuters Foundation is the corporate foundation of Thomson Reuters, the global news and information services company. As an independent charity, registered in the UK and the USA, we leverage our media, legal and data-driven expertise to strengthen independent journalism, enable access to the law and promote responsible business. Through news, media development, free legal assistance and data intelligence, we aim to build free, fair and informed societies.

TrustLaw, an initiative of the Thomson Reuters Foundation, is the world's largest pro bono legal network. Working with leading law firms and corporate legal teams, we facilitate free legal support, ground-breaking legal research and resources for non-profits and social enterprises in over 190 countries. By spreading the practice of pro-bono worldwide, TrustLaw wants to strengthen civil society and drive change. If you have ideas for resources we could develop or legal research projects that would be of assistance after reading this guide, please contact us. If you are a non-profit or social enterprise in need of legal support, you can find out more about the service here and join TrustLaw for free.

Table of contents

REUTERS/Nicky Loh

Executive summary

This report examines the data frameworks of selected jurisdictions for responsible artificial intelligence (AI) systems. With AI technologies advancing rapidly and becoming increasingly embedded in both public and private sectors, it is crucial that data governance frameworks keep pace to ensure ethical, equitable, and human rights–centered AI deployment. The research focuses on six pilot jurisdictions (Chile, Mexico, Kenya, Mauritius, the Philippines, and Taiwan) to explore how their national strategies, laws, and policies around AI align with data regulations and international ethical principles.

The study finds varying levels of regulatory maturity among the jurisdictions, with some, like Taiwan and Chile, integrating strong data protection and governance provisions into their AI frameworks, while others, such as Mauritius and Kenya, are currently relying more heavily on general data protection laws in the absence of AI-specific regulations (although they are working on draft regulatory projects.) Across jurisdictions, common themes include the promotion of transparency, accountability, and non-discrimination, though the degree of enforcement and legal harmonization varies. Many of the jurisdictions reference or incorporate global guidelines, particularly the OECD and UNESCO recommendations, which emphasize privacy, data quality, open data, and human oversight as foundational pillars for trustworthy AI.

The report concludes that while most of the jurisdictions have made initial steps toward aligning AI governance with responsible data use, significant gaps remain (particularly in areas such as biometric data regulation, algorithmic explainability, and impact assessments). Strengthening these frameworks is essential to prevent data misuse, foster public trust, and support the development of AI systems that are fair, inclusive, and beneficial to society.

REUTERS/Noor Khamis

Introduction

Artificial Intelligence (AI) systems are evolving fast and increasingly being deployed by governments and private actors. In this context, governments in different regions are adopting and developing different strategies (documents, regulations, guidelines) to provide an ethical framework for the advancement of AI.

As AI systems are fed with different kinds of data, quality data inputs are required, and data collection processes and access to information should be aligned with data protection laws. Data transparency, protection and democratization will allow for AI systems that are fairer, ethical and focused on human rights compliant.

The aim of the research is to understand the legal frameworks around the use of data, particularly in AI systems, and identify if such regulations are aligned with data protection laws, access to information regulations, data governance, and data sharing principles. For such purposes we have analyzed frameworks in Mexico, Chile, Kenya, Mauritius, Philippines and Taiwan. For this pilot study, we chose two jurisdictions from three different regions as the object of study to provide a snapshot of how the issue is being addressed by different governments. We believe that the work can be replicable and scalable to more countries and regions.

We also intend to see how the strategies of these jurisdictions do or do not align with international ethical principles being developed in data and AI. For this work, we focused on two documents: the OECD Council Recommendations on AI and the UNESCO Recommendation on the Ethics of AI.

The OECD Recommendations emphasize the importance of strong data protection and privacy safeguards (Article 1.2), along with transparency in AI systems through clear disclosure of data sources and processes (Article 1.3). They also stress the need to promote dataset traceability for enhanced accountability (Article 1.5) and encourage responsible data governance to enable ethical sharing (Article 2.2). Additionally, the Recommendations recognize the value of open datasets in driving innovation (Article 2.1) and call for international collaboration to align data governance frameworks and standards (Article 2.5).

The UNESCO Recommendation emphasizes the importance of robust data protection and privacy measures to safeguard personal information throughout the AI system lifecycle. It also highlights the significance of data governance strategies and promotes data traceability and transparency to enhance accountability. The Recommendation calls for international cooperation and identifies "safety and security," "right to privacy, and data protection," and "transparency and explainability" as key principles, forming a policy area for data. It also lists a wide range of personal data and highlights the role of open datasets in driving innovation and AI advancements.

Through a connection facilitated by TrustLaw, the legal pro bono service of the Thomson Reuters Foundation, we asked six pro bono law firms to answer the following questions that guided the research of this study:

- Does the current legal framework related to AI, including laws, draft bills, strategies and regulations, expressly include provisions related to data (such as, data protection principles, data governance, data transparency, open data or data sharing)?

- Based on the above, are data-related provisions included in AI regulations aligned with data protection laws?

- If there are no AI regulations in force or under discussion, do the current regulations or strategies related to data in your jurisdiction apply to the use of data in AI systems (for example, data infrastructure regulations, digital economy or digital transition laws)?

- Has the jurisdiction adopted or incorporated to its legal framework international principles established by the OECD Council Recommendations on AI and/or the UNESCO Recommendation on the Ethics of AI that expressly include provisions related to data protection principles, data governance, data transparency, open data or data sharing?

Through this work we intend to highlight the importance of the right use of quality data for democratic, fair, equitable and unbiased AI systems and we hope that the report will be useful to stakeholders in various sectors.

REUTERS/Ivan Alvarado

Chile

AI frameworks

Chile has had a National Artificial Intelligence Policy since 2021, updated in January 2025. Despite not having a comprehensive AI regulation, at least four proposals have been submitted since 2021 that seek to regulate aspects of AI, which are currently being discussed.

The most recent proposals are:

- Bulletin No. 15935-07,[1] which amends the Criminal Code to punish the misuse of artificial intelligence (entered on May 15, 2023). This bill has a single article, creating a new type of fraud arising through the use, manufacture, or programming of AI. However, it contains no definition of AI for these purposes and is comparable to other means of committing crimes such as using a feigned name or pretending to have assets.

- Bulletin No. 15869-19,[2] which regulates AI systems, robotics and related technologies, in their various fields of application (as of April 24, 2023). The bill defines what it means by AI systems. This same bill adopts the risk-based approach to AI systems followed by the EU AI Act (including the categories of unacceptable risk and high risk), while creating a National Commission on Artificial Intelligence, and establishing obligations for developers, suppliers and users of AI systems.

- Bulletin No. 16021-07,[3] which amends the Criminal Code to incorporate, as an aggravating circumstance of liability, the use of AI in the commission of a crime (filed on June 13, 2023).

- Bulletin No. 16821-19,[4] regulating AI systems, which aims to promote the creation, development, innovation and implementation of AI systems at the service of human beings, which are respectful of democratic principles, the rule of law and the fundamental rights of individuals in the face of the harmful effects that certain uses may have (entered on May 7, 2024).

The next section will delve into the two initiatives most relevant to this study: the AI Policy and the AI and Robotics bill.

1 https://tramitacion.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=15935-07
2 https://tramitacion.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=15869-19
3 https://tramitacion.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=16021-07
4 https://tramitacion.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=16821-19

In October 2021, Chile's Ministry of Science, Technology, Knowledge and Innovation (Minciencia) introduced the country's first National Artificial Intelligence Policy. The policy has four cross-cutting principles and three interdependent aspects, which aim to position Chile as a global leader in AI research, development, and innovation, fostering collaboration and creating new capabilities across various sectors. The policy also emphasizes responsible AI use and sustainable development, aiming to improve the quality of life of Chileans. An accompanying AI Action Plan details the initiatives, responsible parties, and deadlines for implementation over the next decade. This policy was updated in May 2024 to better align it with the recommendations of the Artificial Intelligence Readiness Assessment Report.

The Artificial Intelligence and Robotics Draft Bill, which proposes to regulate AI systems, robotics and related technologies, in their various fields of application, is currently under legislative treatment. According to the provisions of its first article, the bill seeks to promote the creation, development, innovation and implementation of AI systems at the service of human beings, respecting democratic principles, the rule of law and fundamental rights in general.

The proposal, following the structure of the EU AI Act, adopts a "risk-based approach", dividing the different AI models into four categories according to the dangers they present to people. The highest risk level is called "AI systems of unacceptable risk", and models falling into this category are banned. This group includes, among others, subliminal manipulation systems, biometric categorization systems, or systems that rate people's social behavior. For the remaining categories, the draft provides for the imposition of various obligations to ensure the safe operation of AI systems.

Art. 14 of the bill provides for the creation of a Technical Advisory Council on Artificial Intelligence, as a permanent advisory body whose function is to advise the Ministry of Science, Technology, Knowledge and Innovation on matters related to the development, promotion and improvement of AI systems. In addition, the bill proposes various measures to support innovation, encouraging the creation of controlled AI test spaces. In relation to civil liability for damages caused as a consequence of the use of AI systems, Art. 28 establishes that it will be the operator of the system who will have to assume it.

Regarding intellectual property, Art. 23.a of the bill establishes that anyone involved in the application of this law must respect intellectual property rights. Further, Article 31 proposes the amendment of Law No. 17336 on Intellectual Property, introducing in Article 71 a new limit on text and data mining. This allows acts of reproduction, adaptation, distribution or communication to the public without the authorization of the rights holder, provided that the work is accessed in a lawful manner, used for the "extraction, comparison, classification or any other statistical analysis of data", and such use "does not constitute a disguised exploitation [...] of the protected works".

The connection between AI frameworks and data frameworks

From the point of view of data regulation, the AI Policy aims to promote and consolidate a public interest data agenda through different lines of action:

- It is intended to update the regulation of personal data and generate mechanisms that allow adaptation to new technological developments, through the constant legislative developments in matters of personal data.

- It encourages the research and the use of systems that allow data to be processed in a distributed and secure manner, promoting research and development of anonymization techniques, identification of biases, and computer security.

- The Policy seeks to create and consolidate adequate data governance in the State that promotes the availability of quality data. Thus, the Policy recognizes that the State manages a large amount of administrative and population data, which can be used by government agencies, academics and private organizations to generate knowledge and solutions that contribute to the quality of life.

REUTERS/Ivan Alvarado

Regarding the relationship between the regulation of AI contained in the draft law and existing national data rules, the draft law devotes part of its articles to the creation and establishment of guiding principles based on data governance and protection, and the whole of Title VIII to the protection of data confidentiality, as well as sanctions for non-compliance and infringement procedures.

The Bill contemplate privacy and data governance. It is noteworthy that it mentions biometric categorization systems of individuals based on sensitive personal data. Article 3 of the bill include definitions of "Biometric Identification", "Biometric Verification", "Remote Biometric Identification Systems", "Real-time Remote Biometric Identification Systems", "Emotion Recognition System", "Profiling", and "Biometric Categorization". All of which incorporate to the scope of the bill, the regulation of sensitive personal data as biometric information.

For data governance, it mentions adaptation to international security standards, as well as the need to take into account the purpose and context of the AI system.

Article 23 imposes a duty of confidentiality by stating that any natural person, legal entity or State body or agency involved in the application of the present law must respect the confidentiality of information and data obtained from an AI system in the exercise of its functions and activities in such a way as to protect, in particular: (a) Intellectual and industrial property rights and confidential business information or trade secrets of a natural or legal person, including source code; b) Personal data and their processing in accordance with the regulations in force; c) Public interest and national security; and d) The integrity of criminal cases or administrative proceedings.

Article 24 classifies breaches of this duty of confidentiality (into minor, serious and very serious), for the purposes of attending to the powers of the Personal Data Protection Agency, which was created by the approval of the bill that regulates the protection and processing of personal data and creates the Personal Data Protection Agency (Bulletins 11092-07 and 11144-07), while Article 25 regulates the sanctions applicable to each of the breaches according to their level of seriousness.

Article 26 regulates part of the administrative procedure applicable to the imposition of such sanctions, The Personal Data Protection Agency is in charge of hearing such procedure. Article 27 regulates the judicial proceedings of claims against the sanction imposed by the Agency. Finally, Articles 28 and 29 of the draft regulate civil liability incurred for damages arising from the handling or use of an AI system, as well as the procedure applicable to the hearing of such legal actions.

The dialogue with international AI ethical principles

The cross-cutting principles of the AI Policy are as follows:

- AI focused on people's well-being, respect for human rights, and security.
- AI for sustainable development.
- Inclusive AI, with emphasis on the attributes of data integrity and quality in order to recognize and address possible biases. In addition, it highlights the need to develop AI in an inclusive manner, not discriminating and incorporating a gender and cultural diversity perspective, among others.
- Globalized and evolving AI, for the insertion of the country in the global context, promoting participation in bilateral and multilateral spaces, also aligning with Chile's international commitments (such as the OECD Principles on AI).

Thus, the Policy expressly recognizes the principles of the OECD and. the UNESCO Recommendations on AI Ethics, expressly recognizing, among others, the following principles:

- **AI with a focus on the well-being of people, respect for human rights and safety:** It is recognized that AI should contribute to the integral well-being of people. Actions will be oriented towards providing people with a better quality of life, taking advantage of the benefits of AI and addressing its risks and potential negative impacts, with unrestricted respect for the human rights of all citizens. Both the algorithms and the data used to train automated systems, especially when personal data is involved, must be within secure systems. Actions will include risk and vulnerability assessments of these processes to avoid the use of data sets that could lead to arbitrarily discriminatory decisions or results, and to protect critical algorithms that in case of being violated could compromise the security of the country.

- **AI for sustainable development:** AI has great potential for emerging countries, such as Chile, to diversify their economic matrix and make their industries more productive, as well as to foster their ecosystem of research, technology, innovation and the commercial applications derived from it. Thus, actions will be aimed at promoting the use and development of technology in the country, strengthening the ecosystem and incorporating AI as an axis of the country's sustainable development, i.e., with social and environmental considerations.

- **Inclusive AI:** it is enshrined that AI must not discriminate on the basis of protected categories or be used to the detriment of any group. In particular, it is especially important that AI is developed with a gender and sexual diversity perspective, inclusive of historically neglected groups such as indigenous peoples, people with disabilities, or the most

vulnerable sectors of our economy, to become a useful tool for people, ensuring to reduce and close gaps.

The Artificial Intelligence and Robotics Draft Bill, in accordance with the National Artificial Intelligence Policy, includes the following guiding principles in its Article 4, which have been formulated based on the analysis and adoption of the OECD's Recommendations on Artificial Intelligence and UNESCO's Recommendations on AI Ethics. The following principles are listed below:

- **Human intervention and supervision:** AI systems should be developed and used as a tool in the service of human beings, respecting human dignity and personal autonomy, and operating in a way that can be adequately controlled and monitored by human beings.

- **Robustness and** technical **security:** AI systems should be developed and used in a manner that minimizes foreseeable damage, being technically resilient against unforeseen failures such as against attempts to modify the use or performance of the AI system for illicit purposes by third parties.

- **Privacy and data governance:** AI systems should be developed and used in accordance with current privacy and data protection regulations and should only process data that complies with regulations in terms of quality and integrity. Similarly, the data they use should be interoperable.

- **Transparency and explainability:** AI systems should be developed and used by providing adequate traceability and explainability, such that humans can clearly and accurately know and be aware that they are communicating or interacting with an AI system. This is particularly relevant in cases where such knowledge would help them in making decisions about their rights, safety or privacy, informing intended users, where appropriate, how the system has obtained its predictions or results, as well as about the capabilities and limitations of such AI systems.

- **Diversity, non-discrimination and equity:** AI systems will be developed and used throughout their life cycle, in a way that promotes equal access, gender equality and cultural diversity, while avoiding discriminatory effects and selection or information biases that could generate a discriminatory effect.

- **Social and environmental well-being:** AI systems should be developed and used in a sustainable and environmentally and human-friendly manner. Therefore, those responsible for the introduction to the market, commissioning or use of AI systems should review the long-term effects of their application on society, democracy, and the environment.

- **Accountability and responsibility:** AI systems should be auditable and traceable. There should be oversight, impact assessment, audit, and due diligence mechanisms in place to avoid conflicts with human rights norms and threats to environmental wellbeing.

- **Protection of consumer rights:** AI systems should be developed and used in accordance with current regulations on the protection of consumer rights, ensuring fair treatment, delivery of truthful, timely and transparent information and safeguarding freedom of choice and safety in consumption.

REUTERS/Bernardo Montoya

México

AI frameworks

Mexico currently lacks a dedicated legal framework for regulating AI. However, several bills have been discussed in the federal Congress aimed at establishing such regulations. Among these, the four most significant proposals have been the following :

- **Law for the Ethical Regulation of AI and Robotics:**[5] (under discussion in the originating chamber) The bill centers on the following: the creation of Official Standards for AI regulation that are based on ethical principles; the establishment of the Mexican Council of Ethics for AI and Robotics; and the creation of a National Statistical Network for the use and monitoring of AI. It also foresees ethics, respect for human rights, non-discrimination, transparency, personal data protection, gender equality, inclusion of indigenous groups, and respect for intellectual property as guiding principles.

- **The Law that Creates the Mexican Agency for the Development of AI:**[6] (under discussion in the originating chamber) This bill proposes the establishment of a Mexican Agency for the Development of AI as a decentralized public organization under the federal executive branch. Its main functions would include: formulating and implementing a national strategy and policy for AI; promoting activities related to AI in Mexico, including research and development; and establishing principles and responsibilities for the development and use of AI.

- **Federal Law for the Ethical, Sovereign, and Inclusive Development of Artificial Intelligence in Mexico[7] (under discussion in the originating chamber):** The bill proposes the regulation of the development, use and oversight of AI in Mexico through a risk-based classification system; mandates transparency, explainability, and human oversight for automated decisions, especially in sensitive sectors like health, education, and justice; and the creation of a National Council on AI and the National Platform for Algorithmic Auditing to oversee AI governance and ensure accountability. It prohibits AI systems that cause unacceptable harm (mass surveillance, coercive social scoring, or manipulation without consent) and imposes strict liability for high-risk AI.

- **National Law that Regulates the Use of Artificial Intelligence[8] (under discussion in the originating chamber):** The bill identifies key guiding principles for artificial intelligence, including equality of responsibilities, privacy, proportionality, transparency, confidentiality, and usability. It proposes the creation of a National Center for Artificial Intelligence, which would serve as the primary authority on AI-related matters. Additionally, it envisions the establishment of a National Artificial Intelligence System,

5 https://sil.gobernacion.gob.mx/Archivos/Documentos/2023/05/asun_4572130_20230524_1684946286.pdf

6 https://sil.gobernacion.gob.mx/Archivos/Documentos/2023/12/asun_4673074_20231205_1697051780.pdf

7 https://sil.gobernacion.gob.mx/Librerias/pp_ContenidoAsuntos php?SID=5e80326eff046c557bca0d36a76f04e5&Clave=4896460

8 https://sil.gobernacion.gob.mx/Librerias/pp_ContenidoAsuntos. php?SID=5e80326eff046c557bca0d36a76f04e5&Clave=4825444

through which the National Center and other relevant authorities would coordinate efforts and define public policy on AI.

The National Institute for Transparency, Access to Information, and Protection of Personal Data ("INAI", in Spanish) was the autonomous body responsible for ensuring transparency and personal data protection in Mexico. As the data protection enforcing authority, it oversaw AI-related matters, ensuring compliance with privacy regulations, and safeguarding individuals' rights.

In May 2022, the INAI published a document titled "Recommendations for the Treatment of Personal Data Derived from the Use of AI".[9] Although not legally binding, this document offers guidelines for AI development and use by authorities concerning data protection and privacy.

However, it's important to note that the INAI ceased to exist in March 2025 due to a constitutional reform approved in December 2024. Its responsibilities concerning transparency and data protection were transferred to the Ministry of Anti-Corruption and Good Governance.

Currently, there are no court cases related to AI regulations. However, there is an administrative case where the INAI examined the lawfulness of the Tax Ministry's decision for keeping secrecy regarding an AI system used for classifying tax payers for national security purposes.[10] The INAI concluded that the secrecy of this information was lawful.

The connection between AI frameworks and data frameworks

In Mexico, data regulations consist of the General Law on the Protection of Personal Data Held by Mandated Subjects[11] and the Federal Law on the Protection of Personal Data Held by Private Parties[12], along with their respective regulations[13] (collectively referred to as "Data Protection Laws"). This legal framework establishes the following principles for the collection and processing of personal data:

- **Principle of Loyalty:** Personal data processing must prioritize individual interests and reasonable privacy expectations, ensuring trust in the data controller and avoiding deceptive practices.

9 https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/RecomendacionesPDP-IA.pdf

10 INAI's decision can be accessed at the following link: : https://resolucion.inai.org.mx/. Please search for the case file number RRA 4025/24.

11 https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

12 https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

13 https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

- **Principle of Information:** Data controllers must inform individuals of the key characteristics of data processing through a privacy notice, which must be available to all data subjects before processing.

- **Principle of Consent:** Consent is required for processing personal data, except in legally defined exceptions. Consent must be voluntary, informed, and specific to the purposes outlined in the privacy notice.

- **Principle of Proportionality:** Only personal data necessary, appropriate, and relevant to the stated purposes may be processed.

- **Principle of Purpose:** Personal data can only be processed for the purposes specified in the privacy notice.

- **Principle of Quality:** Processed personal data must be accurate, complete, relevant, correct, and up to date to fulfill its intended purpose

- **Principle of Accountability:** Data controllers must ensure compliance with data protection principles and be accountable for the processing of data in their custody or shared with processors.

Importantly, the Data Protection Laws cover a specific category of personal data known as "sensitive data," which includes information that may reveal intimate details about an individual, such as racial or ethnic origin, health status, genetic data, and political opinions. Due to the risks associated with sensitive data, it requires enhanced protection, including explicit written consent for its collection and other obligations.

INAI's decisions have consistently classified biometric14 and financial data as well as data pertaining to children as sensitive[15].

Moreover, when personal data is used in automated decision-making processes without the involvement of a human assessment, Article 112 of the Regulations of the Federal Law on the Protection of Personal Data Held by Private Parties requires that data subjects be explicitly informed of this situation. In such cases, individuals have the right to access their personal data used in the decision and, if any of the data is found to be inaccurate or incomplete, they may exercise their right to rectification. Additionally, the regulations establish that data subjects must be allowed to request a reconsideration of the decision based on the corrected or updated information, ensuring a layer of protection and transparency in the use of automated systems such as artificial intelligence.

To regulate the application of the principles for the collection and processing of personal data in the context of artificial intelligence, the INAI published the "Recommendations for the Treatment of Personal Data Derived from the Use of AI,". This document connected the principles outlined in the Data Protection Laws to the application of AI systems. These recommendations stipulate how to adhere to each principle while handling personal data in AI applications:

| 14 https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf

| 15 https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-178-24.pdf

Principle	Recommendation for AI systems
Principle of Legality	Process personal data in compliance with data protection regulations.
Principle of Loyalty	Do not use deceptive or fraudulent means to collect or process personal data. Respect the individual's reasonable expectation of privacy.
Principle of Information	Provide the privacy notice to individuals before collecting their data. Ensure that the privacy notice includes all required information as per regulations. Write the notice clearly and concisely in plain language for better understanding.
Principle of Consent	Obtain appropriate consent for processing personal data, specifying whether implicit, explicit, or written consent is needed. Request explicit consent for financial or sensitive data. Link consent requests to specific purposes in the privacy notice. Seek new consent for incompatible purposes. Offer easy options for individuals to express consent or refusal.
Principle of Proportionality	Make reasonable efforts to collect only the minimum necessary personal data for the intended purpose of processing. Limit the duration of personal data processing to the minimum necessary period, especially for sensitive data.
Principle of Purpose	Process personal data only for the purposes specified in the privacy notice. Avoid processing personal data for purposes that are incompatible or unrelated to those for which the data was originally collected.
Principle of Quality	Ensure personal data is accurate, complete, and up to date. Retain data only until its purpose is fulfilled, then preserve it. Delete data after the preservation period unless legally required to keep it. Document procedures for retention, blocking, and deletion of personal data.
Principle of Accountability	Private and public sector data controllers must establish procedures to assess and address risks associated with the implementation of new products, services, technologies, and business models that involve data processing, as well as to mitigate identified risks.

Table 1. Data Protection Laws principles' connection to the application of AI systems. Elaborated by Basham Ringe & Correa S.C.

REUTERS/Daniel Aguilar

However, it is currently unclear whether the newly established data protection authority will maintain these interpretative criteria or adopt new standards for classifying sensitive data and regulating the intersection between data protection and AI systems.

Now, each of the main legislative initiatives on AI mentioned above acknowledges the complementary role of the Data Protection Laws. This recognition implies that any collection and processing of personal data in AI systems must align with the broader data protection legal framework, including its guiding principles and specific rules regarding sensitive data.

The Law for the Ethical Regulation of AI and Robotics and the National Law that Regulates the Use of AI acknowledge Data Protection Laws as complementary. This requires the collection and processing of personal data for AI systems to align with this data protection legal framework.

Additionally, alignment with the Data Protection Laws is reinforced by incorporating the requirement to obtain consent for the use of personal data in the Federal Law for the Ethical, Sovereign, and Inclusive Development of Artificial Intelligence in Mexico, as well as explicit prohibitions against using biometric identification without authorization and restrictions on biometric and emotion recognition systems.

Regarding the Law for the Ethical Regulation of AI and Robotics, the initiative addresses the issue of personal data in a limited manner. Nevertheless, it mentions the Federal Law on the Protection of Personal Data Held by Private Parties and the General Law on the Protection of Personal Data Held by Mandated Subjects as supplementary laws.

As for The Bill that Creates the Mexican Agency for the Development of AI, the initiative makes limited references to personal data issues:

- It establishes a working committee on “Privacy and Personal Data”,
- It mentions data protection as a topic to be considered in the National Strategy for AI.

The Federal Law for the Ethical, Sovereign, and Inclusive Development of Artificial Intelligence addresses the matter of personal data by establishing that AI systems must operate in accordance with the broader legal framework governing privacy and data protection. It further states that, in areas not expressly regulated by the law, the applicable legal provisions on personal data, cybersecurity, transparency, and digital rights will apply. Finally, the National Law that Regulates the Use of AI establishes that anyone who uses AI systems must guarantee adequate levels of security to protect personal data and sensible data.

The dialogue with international AI ethical principles

Mexico adopted the UNESCO Recommendation on the Ethics of Artificial Intelligence in November 2021 and the OECD Recommendation on Artificial Intelligence in 2019.

The proposed initiatives include some of the OECD and UNESCO principles for AI, including:

- Promoting the ethical, responsible, and transparent development of AI and a human-centered approach.
- Fostering international cooperation and a participatory multisectoral approach.
- Emphasizing education, human oversight, and the protection of human rights, non-discrimination, and intellectual property.
- Establishing governance mechanisms, such as the National AI Commission, and acknowledging the need to regulate potential risks.

However, while they include some privacy safeguards, like banning unauthorized biometric identification, they fall short on key data governance issues. For example, principles such as explicability specific to the design and operation of AI systems, which are essential to ensuring the protection of data privacy and non-discrimination rights, are absent from the proposed initiatives

In addition, the OECD highlights the need for inclusive AI systems that respect individual rights, but current frameworks lack clear accountability and oversight, undermining public trust and limiting AI's societal benefits. Strengthening these initiatives is crucial for improving data governance and ensuring alignment with OECD and UNESCO's transparency standards.

While the aforementioned draft bills address personal data protection laws, they fall short in adequately safeguarding privacy. AI systems present unique risks to personal data protection that require specific attention. The existing data protection framework does not sufficiently account for the complexities and potential harms associated with AI technologies, such as data misuse, bias, and lack of transparency. To effectively protect individuals' privacy, the legislation must incorporate tailored measures that address these specific challenges posed by AI systems.

Additionally, as mentioned before, a constitutional reform dissolved the INAI and transferred its functions to the Federal Executive branch. This reform shifts the responsibility around access to information and data protection to individual government entities and internal control bodies. These changes are very recent, so the impact of the modifications in practice are yet to be assessed.

REUTERS/Noor Khamis

Kenya

AI frameworks

In Kenya, there is no specific AI regulation but the Data Protection Act addresses some of the data principles and rights of data subjects. However, there is a Bill on AI and a Code of Practice for AI Applications, and a recent National Artificial Intelligence Strategy. The laws, policies, and initiatives that make up the regulatory framework include:

- **Kenya's National Artificial Intelligence Strategy 2025-2030:**[16] The Ministry of Information, Communications, and the Digital Economy has unveiled Kenya's National Artificial Intelligence Strategy for 2025–2030, outlining the country's vision to harness AI for inclusive economic and social development. Built around three core pillars and four supporting ones, the strategy takes a holistic approach to AI integration. The core pillars provide the structural foundation for AI advancement, while the supporting pillars create the enabling environment (addressing essential cross-cutting issues such as regulation, ethics, and capacity building). Together, these seven pillars form a cohesive ecosystem where technological infrastructure is reinforced by human talent, governance frameworks, and ethical safeguards. This integrated approach aims to position Kenya to adopt AI technologies responsibly and effectively, ensuring that innovation goes hand-in-hand with equity, resilience, and public trust. The main pillars are AI digital infrastructure; Data and AI governance; and AI innovation and entrepreneurship. The enabling pillars are Skills development and capacity building; Research and development; International collaboration; and Ethical AI.

- **Taskforce on Distributed Ledgers and Artificial Intelligence:**[17] The Taskforce was created by the Ministry of Information, Communications and the Digital Economy. The mandate of the Taskforce was to: explore and analyze upcoming digital technologies that demonstrate great potential to transform Kenya's economy, including disruptive technologies that are currently shaping the global economy such as distributed ledger technologies (Blockchain and hashgraph), AI, 5G wireless technology, and the internet of things.

- **Kenya Robotics and Artificial Intelligence Society Bill 2023:**[18] The bill proposing the establishment of the Kenya Robotics and Artificial Intelligence Society centers on : promoting the responsible and ethical development and application of robotics and artificial intelligence technologies in Kenya; fostering collaboration and knowledge exchange among robotics and AI practitioners, researchers, and stakeholders; establishing and enforcing standards and best practices for the robotics and AI; and harmonizing the regulation of robotics and AI, including the use of AI in decision-making that could impact people's lives. It entails the principles of public good, human safety

16 https://www.ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf

17 https://kenyanwallstreet.com/kenya-govt-unveils-11-member-blockchain-ai-taskforce-headed-by-bitange-ndemo/

18 https://www.dataguidance.com/sites/default/files/the_kenya_robotics_and_artificial_intelligence_society_bill_2023.docx.pdf

and security, privacy and data protection, accountability and diversity and inclusion in the development and use of robotics and AI.

- **Draft AI Code of Practice by KEBS:**[19] The Kenya Bureau of Standards (KEBS) published the Draft Information Technology Artificial Intelligence Code of Practice (the "Draft AI Code of Practice") on April 8, 2024. The Code was developed to help organizations develop, provide and use AI in a responsible way where the rights of citizens are not compromised while developing AI systems. It includes the following: approaches to establish trust in AI systems through transparency, explainability, controllability, etc.; engineering pitfalls and typical associated threats and risks to AI systems, along with possible mitigation techniques and methods; and approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems. The code is yet to be approved as a national policy guideline.

Some of the other laws that are expected to impact AI include:

- **The Computer Misuse and Cybercrimes Act, 2018:** The Act provides for the protection of critical information infrastructure. Considering the use of computers and devices which are regarded as critical information infrastructure in the generation of AI and related uses, the Act is critical in understanding the obligations of the operators of such information infrastructure.

- **Consumer Protection Act, 2012:** The use of AI by consumers is protected under this general law. Most consumer protection principles on competition, accuracy, services fit for purpose, etc., will be applicable to AI.

The connection between AI frameworks and data frameworks

There is no explicit regulation of the use of data in or for AI systems beyond the principles of public good, human safety and security, privacy and data protection, accountability and diversity and inclusion in the development and use of robotics and AI contained in the Data Protection Act and the Draft AI Code.

However, the use of AI in decision making is prohibited under the Data Protection Act unless it is consented to by the data subject affected by the decision, or as stipulated under the Act.

19 https://www.dataguidance.com/sites/default/files/kebs-tc_094_n66_public_review_kenya_standard_dks_3007_ai_code_of_practice.pdf

The Data Protection Act[20] is data-specific legislation with provisions on the regulation of the processing of personal data, the rights of data subjects and obligations of data controllers and processors. It applies to data entered in a record by making use of automated or non-automated means; establishes the office of the Data Protection Commissioner to oversee the implementation of the Act; and mandates the registration of data controller or data processor. The principles established under Section 25 of the Act include the protection of right to privacy, fairness & transparency in data collection, accuracy, legitimate purpose, and non-transferability outside Kenya.

A notable feature of the proposed Kenya Robotics and Artificial Intelligence Society Bill, 2023 is that it seeks to harmonize the regulation of robotics and AI, including the use of AI in decision-making that could impact people's lives. In doing so, it incorporates some data protection principles, including privacy and data protection.

The Data Protection Act establishes the legal framework for the collection and processing of personal data. The principles contained in the Act include:

- **Principle of Legality:** Personal data must be processed lawfully, fairly, and in a transparent manner in relation to any data subject. The data must also be collected for explicit, specified, and legitimate purposes and not further processed in a manner incompatible with those purposes.

- **Principle of Loyalty:** Personal data must be processed in accordance with the right to privacy of the data subject.

- **Principle of Information:** Data controllers must inform individuals of the key characteristics of data processing through a privacy notice, which must be available to all data subjects before processing. The data must equally be adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed.

- **Principle of Consent:** Consent is required for processing personal data, except in legally defined exceptions. Consent must be voluntary, informed, and specific to the purposes outlined in the privacy notice.

- **Principle of Proportionality:** Only personal data necessary, appropriate, and relevant to the stated purposes may be processed. The same must be kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected.

- **Principle of Purpose:** Personal data can only be processed for the purposes specified in the privacy notice.

- **Principle of Quality:** Processed personal data must be accurate, complete, relevant, correct, and up to date to fulfill its intended purpose. Where necessary, data should be kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay.

| 20 https://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf

- **Principle of Accountability:** Data controllers must ensure compliance with data protection principles and be accountable for the processing of data in their custody or shared with processors.

The dialogue with international AI ethical principles

The Data Protection Act incorporates international principles established by the OECD Council Recommendations on AI and the UNESCO Recommendation on the Ethics of AI that expressly include provisions related to data protection principles, data governance, data transparency, open data and data sharing.

The Data Protection Act contains the principles of protection of right to privacy, fairness & transparency in data collection, accuracy, legitimate purpose and non-transferability outside Kenya.

The Data Protection Act, for instance, requires a data controller or data processor to inform the data subject of the data they seek to collect, the purpose of collecting the same as well as the rights of the data subjects under the Act.

The legality of processing the data is also based on either the consent to the processing for one or more specified purposes; or the necessity to deliver services to the data subject.

The Act also provides that a data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affecting the data subject.

However, the use of AI is permitted where, for instance, the AI-made decision is necessary for entering into, or performing, a contract between the data subject and a data controller; authorized by a law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or based on the data subject's consent.

In terms of open data, portability and sharing, the data subject has a right to receive personal data concerning them in a structured, commonly used and machine-readable format. Additionally, a data subject has the right to transmit the data obtained to another data controller or data processor without any hindrance.

REUTERS/Darrin Zammit Lupi

Mauritius

AI frameworks

There have been concerted efforts to develop strategic plans and rules relating to AI in Mauritius, including the publication of a Mauritius Artificial Intelligence Strategy[21] (the Strategy) with the aim of developing a roadmap on the use of AI in various sectors of the Mauritian economy. The Strategy focuses on the use of AI in various industries and its implications as well as the creation of a legal and regulatory framework to govern AI innovation. One of the key considerations under the Strategy is data protection. The Working Group recognizes that the use of AI has implications for privacy, data protection, and the rights of individuals. A poor legal and regulatory framework may result in data breaches and unintentional release of secure or private and confidential information.

In the wake of the Covid 19 Pandemic, the Data Protection Office has also published a Guide on Data Protection for Health Data and Artificial Intelligence in light of Coronavirus (the Guide).[22] Since AI solutions were being used to contain and forecast the Covid-19 virus, the Data Protection Office shed some light on the application of principles of data protection laws to the use of these AI technologies. Such principles included data anonymization techniques, pseudonymization techniques, purpose limitation, transparency, the right to be informed and time limitation.

The Financial Services (Robotic and Artificial Intelligence Enabled Advisory Services) Rules[23] 2021 (the Rules) were also passed by the Financial Services Commission to regulate services in the Artificial Intelligence and robotics field, which *inter alia* govern: a) the provision of digital and personalized advisory services through a computer program and/or AI-enabled algorithms with limited human intervention - these advisory services are exclusively of financial nature and are related to discretionary and non-discretionary investment and portfolio management services; and b) the creation of a Robotic and Artificial Intelligence Enabled Advisory Services license. Pursuant to the Rules, any person licensed to provide robotic and AI-enabled advisory services has an obligation to preserve the integrity and privacy of their clients' information in conformity with the Data Protection Laws of Mauritius when providing such advisory services.

The Data Protection Act 2017 (the DPA),[24] on the other hand, sets out the general framework applicable to any processing of personal data in Mauritius. Although the DPA does not make any specific reference to AI, the Guide and Rules refer to the general obligations for the preservation of personal data under the DPA.

21 https://mitci.govmu.org/Documents/Strategies/Mauritius%20AI%20Strategy.pdf

22 https://dataprotection.govmu.org/Communique/Guide%20on%20Data%20Protection%20for%20health%20data%20and%20AI.pdf

23 https://www.fscmauritius.org/media/101852/annex-1-128_the-financial-services-robotic-and-artificial-intelligence-enabled-advisory-services-rules-2021.pdf

24 https://dataprotection.govmu.org/Documents/DPA_2017_updated.pdf?csf=1&e=0rlrff

The connection between AI frameworks and data frameworks

While the Strategy provides general guidelines on the use of AI innovation, it does not set out specific data protection rules. On the other hand, the Guide and the Rules refer to the DPA (details of these data protection principles are set out below) in terms of handling personal data. The DPA is aligned with the European Union's General Data Protection Regulation (GDPR).

In 2018, in addition to the Guide, the Ministry of Technology, Communication and Innovation also launched the Digital Government Transformation Strategy 2018-2022 (the Transformation Strategy),[25] and the Digital Mauritius 2030 Strategic Plan[26] (the Strategic Plan) to support the country in its pursuit of digital transformation. The DPA remains the overarching law in respect of the processing of data under the Transformation Strategy and the Strategic Plan.

Mauritius has also ratified the Malabo Convention (African Union Convention on Cybersecurity and Personal Data Protection) in 2017 and the Convention 108+ in 2020 to protect the right to privacy of individuals.

As mentioned, the DPA regulates the processing of personal data in Mauritius. Personal data is defined as any information relating to a data subject i.e. an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

The DPA also defines special categories of personal data that require additional safeguards. These include information about a person's racial or ethnic origin, political opinions or affiliations, religious or philosophical beliefs, trade union membership, physical or mental health status, sexual orientation, sexual practices or preferences, as well as genetic and biometric data that uniquely identify an individual. The DPA also considers data related to criminal matters as sensitive (this includes criminal acts a person is accused or convicted of and any legal proceedings involving alleged or actual offences committed by them, including the outcome of such proceedings or any sentence imposed by a court).

25 https://mitci.govmu.org/Documents/Strategies/Final%20Digital%20Government%20Transformation%20Strategy%202018%20-%202022.pdf

26 https://mitci.govmu.org/Documents/Strategies/DM%202030%2017%20December%202018%20at%2012.30hrs.pdf

Any person who wishes to process personal data of a data subject for use in an AI system has to comply with the principles relating to the processing of personal data as set out under the DPA. Such principles include but are not limited to:

- the lawful processing of personal data in a fair and transparent manner;
- collection of personal data for explicit, specified and legitimate purposes;
- the personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed; and
- the personal data shall be accurate and where necessary, kept up to date.

In order for the processing of personal data to be lawful, it must have a legal basis. Accordingly, no person shall process personal data of a data subject unless:

- the data subject consents to the processing for one or more specified purposes;
- the processing is necessary–
    - for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
    - for compliance with any legal obligation to which the controller is subject;
    - in order to protect the vital interests of the data subject or another person;
    - for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    - the performance of any task carried out by a public authority;
    - the exercise, by any person in the public interest, of any other functions of a public nature;for the legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
    - for the purpose of historical, statistical or scientific research.

The DPA provides for further requirements in the context of the processing of special categories of personal data.

A data subject also has a right of access, rectification and erasure of its personal data and the right to object to the processing of his personal data in accordance with the DPA.

Although not part of the legislation, it is also worth noting that the Guide issued by the Data Protection Office (DPO) also provides a list of recommendations when using AI especially for health-related data. These revolve around 6 recommendations as follows:

- **Data anonymization:** The DPO encourages the use of anonymisation techniques to study large group movements effectively without revealing personal identities.
- **Pseudonymization:** The DPO recommends the implementation of pseudonymisation algorithms to ensure sensitive information, such as COVID-19 patient data, remains non-identifiable while sharing relevant data.
- **Purpose limitation:** the data processor must ensure that personal data collected for public health purposes is not repurposed for unrelated uses that conflict with its original intent.
- **Transparency:** the DPO recommends data processors to maintain clear communication with individuals regarding the processing of their data by providing comprehensive yet simple explanations about what data is collected, the underlying logic, and potential outcomes of automated AI decisions.
- **Right to be informed:** the data processors should inform individuals about the types of data collected, the purpose of processing, data-sharing details, storage duration, and whether the data submission is voluntary or mandatory.
- **Time limitation:** the DPO also recommends that post-crisis, the authorities should reassess the technologies deployed to prevent long-term infringements on privacy and ensure that temporary measures do not become permanent norms.

REUTERS/Ed Harris

The dialogue with international AI ethical principles

As at date, Mauritius has not expressly adopted or incorporated international principles established by the OECD Council Recommendations on AI or the UNESCO Recommendation on the Ethics of AI to its legal framework. Although the government expressed its plan to establish a Mauritius Artificial Intelligence Council (MAIC) as part of the Strategy, no action has been taken so far.

However, there are similarities between the UNESCO Recommendation on the Ethics of AI and the DPA with respect to the following:

- the implementation of adequate data protection frameworks and governance mechanisms regarding the collection, use and disclosure of personal data and exercise of their rights by data subjects;
- ensuring a legitimate aim and a valid legal basis for the processing of personal data, including informed consent; and
- privacy impact assessments.

The OECD Council Recommendations on AI, the UNESCO Recommendation on the Ethics of AI, the Strategy, the Transformation Strategy and the Strategic Plan also have certain pillars in common which include transparency, the creation of a data-driven culture, international cooperation and the implementation of legal and regulatory frameworks.

REUTERS/Darren Whiteside

Philippines

AI frameworks

While the Philippines has a general data privacy legislation, it does not have an AI-specific legislation in place to date.

On 19 December 2024, the National Privacy Commission ("NPC") issued an advisory ("NPC Advisory No. 2024-04") concerning the use of AI systems for processing personal data. It is not legislation, but an administrative issuance which provides further guidance regarding the application of general privacy principles insofar as AI systems involve the processing of personal data.

There are also house bills ("HB" or "Bill"), and draft regulations that include provisions directly related to data protection measures and principles.

Key initiatives and legislative proposals concerning the use of AI include the following:

- **NPC Advisory No. 2024-04:** This advisory clarifies the applicability of the Republic Act ("RA") No. 10173, and the Data Privacy Act of 2012 (the "DPA"), including its implementing regulations, as well as the principles of data privacy therein, and the processing of personal information for the development or deployment of AI systems, including its training and testing. The advisory sets out principles and measures that personal information controllers ("PICs") and personal information processors ("PIPs") should follow in using and processing personal information for the development of AI systems, and how the general principles of data privacy should be applied to AI. Some applications of the principles recommended by the advisory include:
    - **Transparency:** This entails informing data subjects of the purpose and extent of processing of personal data through the AI system, as well as the risks and dispute mechanisms present.
    - **Accountability:** PICs and PIPs are accountable for the processing of AI systems and for the outcomes and consequences of such processing when personal data is involved. PICs and, in cases where the processing is subcontracted or outsourced, their PIPs, must be able to demonstrate that they have implemented effective policies and procedures to comply with the DPA and other advisories of NPC. PICs are also required to institute appropriate and effective governance mechanisms to ensure the responsible and ethical processing of personal data in the development or deployment of AI systems, including its training and testing.
    - **Fairness:** PICs must ensure that personal data is processed in a manner that is neither manipulative nor unduly oppressive to data subjects. In this regard, PICs must consider systemic bias, human bias, and statistical bias when assessing or auditing their AI systems.
    - **Accuracy:** PICs must maintain the accuracy of personal data to ensure the fairness of the output of the AI systems.

- **Data Minimization:** PICs must maintain the accuracy of personal data to ensure the fairness of the output of the AI systems.
- **Lawful Basis for Processing:** PICs should determine the most appropriate lawful basis under Sections 12 and 13 of the DPA prior to the processing of personal data in the development or deployment of AI systems, including its training and testing. The advisory also provides that rights of data subjects also apply to those whose personal data are used for AI development, and mechanisms that PICs should put in place to ensure these rights.

- **HB No. 7396:** An Act Promoting the Development and Regulation of Artificial Intelligence in the Philippines:[27] the "Artificial Intelligence Development and Regulation Act of the Philippines" aims to promote and regulate the deployment of AI technologies in the Philippines to ensure that AI systems are developed, deployed, and used in a manner that is "consistent with ethical principles, protects human rights and dignity, and serves the public interest." The Bill proposes the creation and establishment of an AI Development Authority ("AIDA"), an AI regulatory body with the authority to oversee the development and deployment of AI technologies, ensuring compliance with AI ethics principles and guidelines, and protecting the rights and welfare of individuals and communities affected by AI technologies. The AIDA is to be composed of permanent board members and *ex-officio* members, with permanent board members comprising several representatives from the Philippine government, one representative each from the private sector and the academia, both of whom must be an expert in the field of information technology and specializing in AI, law, ethics, social science, and other relevant disciplines. The AIDA will be responsible for, among others: (i) developing a national AI development and regulation strategy that aligns with national priorities and international standards, including requirements for AI impact assessments, data protection, and transparency in AI decision-making; (ii) ensuring that personal data collected, used, and processed by AI systems are protected in accordance with the DPA and other relevant laws and regulations, and (iii) developing data security and cybersecurity standards for AI systems to protect against cyber-attacks and hacking.

- **HB No. 7913:**28:An Act Establishing a Regulatory Framework for a Robust, Reliable, and Trustworthy Development, Application, and Use of Artificial Intelligence (AI) Systems, Creating the Philippine Council on Artificial Intelligence, Delineating the Roles of Various Government Agencies, Defining and Penalizing Certain Prohibited Acts: HB No. 7913, or the "Artificial Intelligence (AI) Regulation Act" aims to regulate the transfer and promote the adaptation of technology from all sources for national benefit, through the pursuit of the development of AI, including digitization and infrastructure, workforce development, research and development, with the end view of harnessing AI's potentials to uplift the lives of Philippine citizens, local industries, and the economy. The Bill proposes an "AI Bill of Rights," which provides Philippine citizens the following rights: (i) right to protection from unsafe and ineffective systems, (ii) right against algorithmic discrimination, (iii) right to privacy, (iv) right to know, and (v) right to remedy.

| 27 https://docs.congress.hrep.online/legisdocs/basic_19/HB07396.pdf
| 28 https://docs.congress.hrep.online/legisdocs/basic_19/HB07916.pdf

Specifically, the right to privacy provides: *"Every person shall be protected from violations of privacy through design choices that ensure such protections are included by default. Data collection that conforms to reasonable expectations and that only data strictly necessary for the specific context is collected shall be ensured. Designers, developers, and deployers of AI systems shall seek permission and respect the decisions of every person regarding collection, use, access, transfer, and deletion data in appropriate ways and to the greatest extent possible. Alternative privacy by design safeguards shall be used whenever applicable. Systems shall not employ user experience and design decisions that obfuscate user choice or burden users with defaults that are privacy invasive. Consent shall only be used to justify collection of data in cases where it can be appropriately and meaningfully given."*

The Bill also proposes the creation and establishment of a "Philippine Council on Artificial Intelligence," ("PCAI" or "Council") which is to be a policy-making and advisory body of experts under the Department of Science and Technology ("DOST"). The "core committee" of the Council will be composed of an AI researcher, robotics specialist, a machine learning expert, a data science specialist, a technology expert, an ethicist, a sociologist or anthropologist, a psychologist, a public health expert, a security analyst, a legal scholar, a human rights advocate, a citizens' representative, and such other experts that the President of the Philippines may appoint.

The Council has the power to, among others, (i) promulgate rules to prevent abusive and harmful applications of AI, (ii) ensure an efficient balance in the regulation of AI and consumer protection to facilitate the growth of emerging business models brought about by AI utilizing regulatory sandbox approach to reduce the cost of innovation and barriers to entry, including the collection of data and information regarding appropriate regulatory action, and (iii) build an AI ecosystem culture by strengthening intellectual property and data protection measures.

The Bill also proposes to prohibit (i) persons from using AI systems that cause "unnecessary, unjustifiable and indiscriminate moral or pecuniary damage to individuals," (ii) the use of lethal autonomous weapon systems, (iii) the development, application, and use of AI to manipulate, exploit or control any person beyond his or her consciousness to materially distort his or her behavior in a manner likely to cause the person physical or psychological harm, (iv) AI-based social scoring of natural persons, and (v) practices that undermine privacy rights.

- **DTI National Artificial Intelligence Strategy Roadmap:**[29] On May 5, 2021, the Department of Trade and Industry ('DTI') launched the National AI Strategy Roadmap (the "Roadmap"), to guide government and private sector stakeholders in employing AI technologies and developing AI economies, while being mindful of its potential consequences.

One of the main recommendations under the Roadmap is the establishment of the National Center for AI Research ("NCAIR"), which will serve as the country's shared hub for AI research to support the digital transformation of the country's enterprises and industries[30]. The NCAIR will be responsible for advancing scientific discoveries in AI, including algorithmic innovations, developing AI talent, and engaging in research and development projects.

29 https://drive.google.com/file/d/1de5kfaGi3tdUgxu1UPV8iRxKpXECTkDp/view

30 DTI to launch National Artificial Intelligence Roadmap, 5 May 2021, available at https://www.dti.gov.ph/archives/national-artificial-intelligence-roadmap/

The Roadmap is organized according to pillars, strategic dimensions, strategic imperatives, and strategic tasks. In relation to data, there is a strategic imperative to improve data access and data value extraction, which includes, among others, the following strategic tasks:

- Make public data open, available, and digestible, for analysis.
- Build a National Data Center that will be a one-stop-data-shop for governments, universities, and enterprises, and will eventually be housed under the proposed National Center for AI Research.
- Invest in a National Research Cloud that will be part of NCAIR, which will afford scientists and researchers with low-cost access to computing power and public datasets secured in a cloud environment.
- Encourage and promote data analysis (at least descriptive analytics) across all functions of businesses, industries, and government agencies.
- For more sensitive data sets, promote projects that would enable access to them as long as the business value and/or the value to society is clear.

There are also strategic tasks to promote data literacy, increase business analytics, data science, and AI graduate students; include data science and analytics as general education courses in universities; incentivize industries to offer data literacy; and establish a committee of experts in data and AI ethics.

On July 3, 2024, the DTI launched the National AI Strategy Roadmap 2.0 and the Center for AI Research ("CAIR"). This updated Roadmap incorporates recent technological advancements, including generative AI, and recalibrates strategic actions to address emerging themes such as ethics and governance[31].

Other initiatives include:

- **HB No. 7983:** An Act Providing a National Strategy for the Development of Artificial Intelligence, Creating for the Purpose the National Center for Artificial Intelligence Research, and Appropriating Funds Therefor;[32]
- **HB No. 10385:** An Act Promoting the Development and Regulation of Artificial Intelligence in the Philippines;[33]
- **HB No. 10944:** An Act Establishing a Regulatory Framework for a Reliable and Secure Development, Research, Application, and Use of Artificial Intelligence (AI) Systems, Creating the Philippine Artificial Intelligence Board, Delineating the Roles of Various Government Agencies, Defining and Penalizing Certain Prohibited Acts;[34]

31 DTI launches National AI Strategy Roadmap 2.0 and Center for AI Research, positioning the Philippines as a Center of Excellence in AI R&D, 03 July 2024, available at https://www.dti.gov.ph/archives/news-archives/dti-launches-national-ai-strategy-roadmap-2-0-center-ai-research-positioning-philippines-center-excellence-ai-rampd/

32 https://docs.congress.hrep.online/legisdocs/basic_19/HB07983.pdf

33 https://docs.congress.hrep.online/legisdocs/basic_19/HB10385.pdf

34 https://docs.congress.hrep.online/legisdocs/basic_19/HB10944.pdf

- **HB No. 10751:** An Act Mandating the Department of Education, Commission on Higher Education, Department of Science and Technology and Department of Information and Communication Technology to Develop Generative Artificial Intelligence (GenAI) Regulations to Maximize its Positive Impact on Philippine Education System;[35]
- **HB No. 10845:** An Act Establishing a Comprehensive Framework for the Integration of Artificial Intelligence in Government Transaction and Processes, and for Other Purposes;[36]
- **HB No. 9448:** An Act Regulating the Use of Artificial Intelligence and Automation Systems in the Labor Industry and for Other Purposes;[37] and
- DICT and Civil Service Commission ("CSC") Draft Joint Memorandum Circular Principles and Guidelines for an Ethical and Trustworthy Use of Artificial Intelligence in the Government


REUTERS/Darren Whiteside

| 35 https://docs.congress.hrep.online/legisdocs/basic_19/HB10751.pdf
| 36 https://docs.congress.hrep.online/legisdocs/basic_19/HB10845.pdf
| 37 https://docs.congress.hrep.online/legisdocs/basic_19/HB09448.pdf

The connection between AI frameworks and data frameworks

To date, there are no data regulations that specifically relate to AI that are currently in force in the Philippines. The Bills mentioned in the previous session are all pending before the Philippine Legislature.

However, it appears that the data-related provisions in the Bills are aligned with the DPA and its implementing rules and regulations ("DPA IRR"), given that these provisions either make express reference to the DPA or operate under the DPA and the DPA IRR's regulatory framework.

The current regulations related to data protection in the Philippines apply to the use of data in AI systems, particularly in the context of processing data using automated decision-making.

Automated decision-making refers to "a wholly or partially automated processing operation that can make decisions using technological means totally independent of human intervention." One type of automated decision-making is profiling, which refers to the "use of personal data, such as an individual's economic situation, political or religious beliefs, behavioral or marketing activities, personal preferences, electronic communication data, location data, and financial data, among others, in order to evaluate, analyze, or predict his or her performance, qualities, and behavior, among others." AI systems may fall under the above definitions, and therefore be governed by data privacy rules.

Pursuant to the DPA and DPA IRR, the National Privacy Commission ("NPC"), the government agency mandated to implement the DPA, issued the following circulars with provisions relating to automated decision-making and profiling:

- **NPC Advisory No. 2024-04:** (analyzed in the previous section)
- **NPC Circular No. 2022-04 - Registration of Personal Data Processing System, Notification Regarding Automated Decision-Making or Profiling, Designation of Data Protection Officer, and the National Privacy Commission Seal of Registration:** This circular provides that data processing systems processing personal or sensitive personal information involving automated decision-making or profiling should, in all instances, be registered. Thus, the use of AI in processing data, if it is totally independent of human intervention, will trigger the mandatory registration requirements of the NPC.
- **NPC Advisory No. 2021-01 - Data Subject Rights**[38]**:** Under this advisory, the data subject has the right to be informed whether personal data pertaining them has been, is, or will be processed, including the existence of automated decision-making and profiling. Data subjects also have the right to object to the processing of their personal

| 38 https://www.privacy.gov.ph/wp-content/uploads/2021/02/NPC-Advisory-2021-01-FINAL.pdf

data, for direct marketing, profiling, or in cases of automated processing where the personal data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect them.

- **NPC Circular No. 2023-04 - Guidelines on Consent:**[39] This circular requires a personal information controller ("PIC") to obtain the consent of the data subject when automated processing is the sole basis for a decision that produces legal effects on or may significantly affect the data subject. PICs must also inform the data subject of the existence and specific details of the profiling or automated processing of personal data before its entry into the processing system. The PIC must ensure that there are safeguards against the harms of extensive profiling such as discriminatory outcomes and infringement on the right to fair treatment.

- **NPC Advisory No. 2023-01 - Guidelines on Deceptive Design Patterns:**[40] This advisory provides guidance on PICs on the nature of deceptive design patterns, and their impact on the lawful processing of personal data based on the data subject's consent. "Deceptive Design Patterns" refer to design techniques embedded on an analog or digital interface that aim to manipulate or deceive a data subject to perform a specific act relating to the processing of their personal data. Given the applicability to digital interfaces, PICs using AI systems should ensure transparency in the presentation of information to the data subject by avoiding deceptive design patterns. Additionally, the digital interface must be designed and operated in a way that the processing of information will not be detrimental, discriminatory, unexpected, or misleading to a data subject.

- **Cybercrime Prevention Act of 2012:** There is a law on cybercrime prevention that may generally apply to AI systems. The Cybercrime Prevention Act of 2012 enumerates acts which constitute cybercrime offenses. Particularly, offenses against the confidentiality, integrity and availability of computer data and systems include (i) illegal access, (ii) illegal interception, (iii) data interference, and (iv) system interference.

39 https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Circular-No.-2023-04_Guidelines-on-Consent_07Nov2023.pdf

40 https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Advisory-No.-2023-01-Guidelines-on-Deceptive-Design-Patterns_7Nov23.pdf

The dialogue with international AI ethical principles

At present, the administrative issuance sets out principles and measures that PICs and PIPs should follow in using and processing personal information for the development of AI systems, and how the general principles of data privacy should be applied to AI is NPC Advisory No. 2024-04. The issuance broadly adopts the principles of transparency and accountability established in the OECD Council Recommendations on AI and the UNESCO Recommendation on the Ethics of AI. NPC Advisory No. 2024-04 and the DPA emphasize the protection of data privacy, in alignment with the fundamental principles outlined in the UNESCO Recommendation on the Ethics of AI to safeguard the right to privacy. NPC Advisory 2024-04 mandates that PICs establish systems enabling significant human intervention performed by individuals with the required expertise and authority. This closely corresponds with the necessity for human oversight as stated in the UNESCO Recommendation on the Ethics of AI.

The Government, via the National AI Strategy Roadmap 2.0, implemented policies that emphasize research and development in AI in line with the OECD Council Recommendations on AI.

The abovementioned draft of the Principles and Guidelines for an Ethical and Trustworthy Use of Artificial Intelligence in the Government, by DICT and CSC, aims to provide the basic principles and guidelines for ethical and trustworthy use of AI in government, adopting the OECD AI Principles that "AI should be innovative and trustworthy and respect human rights and democratic values." In particular, principles mentioned include: Principle of Do No Harm; Cyber Safety and Security; Data Privacy and Protection; Robustness and Reliability; Fairness and Non-Discrimination; Transparency and Explainability; Responsibility and Accountability; Contestability; Reasonable Human Control; Human-centricity; Sustainability.

While not AI-centric, R.A. No. 11927, commonly referred to as the Philippine Digital Workforce Competitiveness Act, was established to form an Inter-Agency Council aimed at enhancing the digital skills of all working-age citizens and providing them with digital competencies, which encompass digital entrepreneurship and remote work utilizing digital skills, to capitalize on the expanding job opportunities and advantages presented by digital technologies. This aligns with the OECD Council Recommendations on AI, especially regarding the enhancement of human skills and readiness for changes in the labor market.

REUTERS/Nicky Loh

Taiwan

AI frameworks

Starting from 2023 to date, Taiwan is shaping its legal framework for AI through several existing and draft non-binding guidelines, as well as a draft of the AI Basic Act ("Draft AI Basic Act"). Most of the regulations provide high-level principles and ethical considerations, and neither the Draft AI Basic Act nor the non-binding guidelines grant enforcement power to competent authorities or impose mandatory obligations on the private sector. Meanwhile, once the Draft AI Basic Act is enacted, authorities are expected to formulate sector-specific AI regulations.

The guidelines currently in effect include the following:

- **AI Technology R&D Guidelines:**[41] In September 2019, the Taiwan National Science and Technology Council ("NSTC") issued the AI Technology R&D Guidelines, which aim to promote ethical research in AI technology.
    - The guidelines emphasize AI safety, which includes system robustness, network security, information security, and risk control and monitoring. (Point 4)
    - The guidelines enshrine the importance of privacy and data governance by requiring internal data management systems and legal compliance with laws for data collection, processing, and usage. (Point 5)
    - In addition to the requirement of transparency in modules, mechanisms, components, parameters, and calculations, the guidelines also emphasize traceability of decisions, including proper documentation of data collection, data labeling, and algorithms. (Point 6)
    - The guidelines require that AI users and those affected by AI be informed of, shown, and explained the AI system, software, and algorithm after the use. (Point 7)
    - Accountability should be ensured. (Point 8)
- **Guidelines for Use of Generative AI by the Executive Yuan and its Subordinate Agencies ("Public Sector Gen AI Guidelines"):**[42] The NSTC promulgated the Public Sector Gen AI Guidelines in 2023 to establish a framework for the ethical application of generative AI within the public sector.
    - Confidential information, including personal data and undisclosed official data, must not be shared with generative AI systems unless deployed in a secure, closed environment where information is at a certain level of confidentiality. Generative AI systems should not be asked questions related to confidential matters or personal information. (Point 4)

| 41 https://www.nstc.gov.tw/nstc/attachments/53491881-eb0d-443f-9169-1f434f7d33c7

| 42 https://www.nstc.gov.tw/folksonomy/list/c79bf57b-dc94-4aff-8d14-3262b5559cfc?l=ch

- Any use of generative AI to assist government operations or public services must be disclosed appropriately. (Point 6)
- Any use of generative AI should comply with cyber security, personal data protection, copyright, and information usage regulations. (Point 7)

- **Guidelines for the Use of AI in the Financial Industry[43] ("Financial AI Guidelines"):** The Financial Supervisory Commission ("FSC") released the Financial AI Guidelines on June 20, 2024. The Financial AI Guidelines provide detailed instructions for financial institutions to follow when using AI.

  - One of the core principles is to protect customers' privacy and interests. Financial institutions should ensure that the AI system complies with the PDPA and its internal data policies across each stage of the AI lifecycle. In addition to following the data minimization principle, financial institutions are required to properly process customers' data; measures such as encryption, secure access controls, and regular monitoring are suggested. (Chapter 3)
  - Financial institutions should ensure the robustness and safety of the AI system. They should take measures to prevent security threats and attacks. (e.g., hacker attacks and malware). (Chapter 4)
  - Financial institutions are required to disclose AI systems' use of data, the basis for decision-making, and the potential impacts on stakeholders. Maintaining traceability through thorough documentation of data sources, processing methods, and outputs is critical for accountability and regulatory compliance. (Chapter 5)

In addition to the above guidelines that are already in effect, there are also the following proposals:

- **The Draft AI Basic Act:**[44] The NSTC announced the Draft AI Basic Act for public comment on July 15, 2024; the draft is still being discussed by the Executive Yuan (Taiwan's cabinet) and has not yet been reviewed by the Legislative Yuan (Taiwan's parliament). The Draft AI Basic Act aims to establish a governance framework for the development and use of AI technology.

  - Data protection principles are outlined for the government to follow in advancing AI research and development. These principles include privacy protection and data governance, information security and safety, and transparency and explainability. Accountability is also listed as one of the principles. (Article 3)
  - It requires the government to develop an AI risk classification framework in alignment with international standards for the development of AI information security, risk classification, and risk management (similar to the European Union's AI Act). (Article 10)

43 https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202406200001&dtable=News

44 https://join.gov.tw/policies/detail/4c714d85-ab9f-4b17-8335-f13b31148dc4

  - It requires the competent authority of the Personal Data Protection Act ("PDPA") to assist sectoral regulators in ensuring data minimization and promoting data protection by default and by design. (Article 14)
  - It requires establishing systems for data openness, sharing, and reuse. (Article 15)

According to the NSTC, the structure and content of the Draft AI Basic Act aim to strike a balance between the innovation-driven regulatory approach of the United States and the rights-protection-focused regulatory approach of the European Union[45].

- **Draft Public Sector AI Playbook:**[46] On December 20, 2024, the Ministry of Digital Affairs ("MODA") issued the Draft Public Sector AI Playbook, which will undergo a one-year trial period from January 1 to December 31, 2025. The draft playbook provides authorities with guidance and suggestions for building AI services. The draft playbook identifies data security and information security as important issues for AI operations.
  - The use of sensitive data should be subject to data protection laws and limited to the scope of specific purposes. Lawfulness, purpose limitation, transparency, the right to opt-in, the right to opt-out, data minimization, storage limitation, and security should be controlled. Also, authorities should avoid storing large amounts of sensitive data for long periods of time without purpose of use. (Chapter 4.3)
  - The playbook outlines key information security concerns, emphasizing risks such as data leakage, data poisoning, reverse engineering, and prompt injection attacks. To mitigate these risks, it recommends strict security compliance, avoiding unverified AI tools, limiting AI automation without human oversight, and using Privacy Enhancing Technologies (PET) for secure API connections. (Chapter 4.4)
- **Draft Guidelines for the Evaluation of AI Products and Systems ("Draft AI Evaluation Guidelines"):**[47] In March 2024, MODA announced the Draft AI Evaluation Guidelines, aiming to assist industries by providing them with a document to comply with when they develop or utilize AI products and systems. The Draft AI Evaluation Guidelines encourage industries to self-monitor their AI products or systems based on risk levels.
  - Referencing the EU AI Act, the Draft AI Evaluation Guidelines classify AI products and systems into four risk levels and provide specific criteria for evaluating AI products; the criteria include transparency, privacy, and data security.
  - The guidelines also recommend measures to be adopted. For example, industries should establish privacy and data security safeguards, record the usage of sensitive personal data, review third-party material to assess risks of privacy and security, and continuously monitor the security of AI products or systems.

45 https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

46 https://moda.gov.tw/digital-affairs/digital-service/guide/15002

47 https://moda.gov.tw/ADI/news/bulletin-board/11896

REUTERS/Richard Chun

The connection between AI frameworks and data frameworks

Data protection in Taiwan is primarily governed by the PDPA[48] and the Enforcement Rules of the PDPA.[49] All the data-related provisions included in AI regulations require compliance with the PDPA or data protection laws. Specifically, Article 14 of the Draft AI Basic Act directly states that the competent authority of the PDPA should assist sectoral regulators in creating mechanisms or measures for data protection. This demonstrates that the Draft AI Basic Act is designed to implement PDPA standards with regards to AIstate that institutions should ensure the AI system is consistent with the PDPA. As for the other non-binding guidelines and playbook, while those do not specifically refer to the PDPA, compliance with "data protection laws" is also required.

It may be argued that the current PDPA is insufficient for AI practices, and examples include as follows:

- Biometric data has not been listed as sensitive data under the PDPA. Moreover, the PDPA does not apply to biometric data that is collected, processed, or used in public places or public activities and not connected to other personal data. AI's large-scale utilization of facial recognition in public may not be covered.

- The PDPA lacks a data protection impact assessment mechanism for new technologies such as AI.

- The PDPA lacks protection measures concerning automated decision-making (including profiling) and the right to data portability, which could be critical in AI data collection.

In response to the development of digital technologies such as AI, the Executive Yuan established the "Digital Policy and Legal Affairs Coordination Committee" in 2023. This cross-ministerial platform collects, analyzes, and coordinates digital legal issues among various government agencies. Among them, the Preparatory Office for the Personal Data Protection Commission (i.e., the competent authority of the PDPA) is responsible for the legal frameworks on personal data in relation to digital technologies and AI. Therefore, new legal amendments addressing AI-related issues can be fairly expected in the near future.

Other than the AI-related regulations previously discussed, Taiwan's current regulations governing data do not regulate AI directly. However, they remain applicable to the utilization of data within AI systems whenever such utilization pertains to the behaviors, industries, or sectors already covered by the existing regulations and strategies. In other words, AI serves merely as a tool employed by regulated entities, and emphasis remains on governing the actions and consequences that arise from its use.

| 48 https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021

| 49 https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050022

For instance, under the PDPA, if the use of data, irrespective of the medium in which the AI is included, involves the collection, processing, or utilization of personal information that can be used to directly or indirectly identify a specific data subject, the PDPA applies. According to the Interpretative Letter No. FLZ-10703512280 issued by the Ministry of Justice in September 2018[50], the PDPA is applicable to the processing of medical imaging data containing special personal information for AI purposes, affirming that data usage in AI is subject to the PDPA.

Regarding data infrastructure regulation, if the AI user is a government agency or a designated non-government agency (i.e., critical infrastructure provider), the Cyber Security Management Act[51] is applicable. Specifically, regulated entities are required to stipulate, amend, and implement a cyber security maintenance plan; additionally, reporting and response mechanisms are required.

The dialogue with international AI ethical principles

The OECD Recommendations are directly mentioned in the preamble of the Draft AI Basic Act, indicating Taiwan's legal framework has taken into account the OECD Recommendations and should be aligned with them.

The Draft AI Basic Act has integrated elements of international principles that align with the OECD Recommendations.

- **Data Protection Principles:** Item 3, Article 1 and Article 14 of the Draft AI Basic Act emphasizes the safeguarding of personal data privacy, adopting the principles of "data protection by design and by default," and minimizing unnecessary data collection. The Draft AI Basic Act also enshrines the importance of information security, which aligns with OECD principles regarding privacy and data protection (Article 1.2 of the OECD AI Principles).

- **Data Governance:** Article 14 of the Draft AI Basic Act promotes the establishment of mechanisms for data governance within authorities to ensure the safe and ethical use of data. This is consistent with the OECD's emphasis on data governance frameworks (Article 2.2 of the OECD AI Principles).

- **Data Transparency:** Item 5, Article 3 of the Draft AI Basic Act mandates transparency and explainability in AI outputs to ensure that stakeholders comprehend the sources and rationale behind AI decisions. This reflects OECD principles advocating for

| 50 https://mojlaw.moj.gov.tw/LawContentExShow.aspx?id=FE315623&type=E&keyword=&etype=etype5

| 51 https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297

responsible disclosure (Article 1.3 of the OECD AI Principles).

- **Open Data and Data Sharing:** Article 15 of the Draft AI Basic Act requires the establishment of mechanisms for data openness, sharing, and reuse to enhance data availability for AI development. This aligns with the OECD's recommendations regarding open datasets as a means to foster innovation and an AI-enabling ecosystem (Article 2.1 and Article 2.2 of the OECD AI Principles).

While the UNESCO Recommendation was not mentioned in the documents related to the Draft AI Basic Act, Taiwan's legal system also contains most of the principles therein.

Also taking the Draft AI Basic Act as an example, most of the international principles listed in the UNESCO Recommendation are basically covered by Taiwan's legal framework:

- **Data Protection Principles:** All the principles highlighted in the UNESCO Recommendation are named in Article 2 of the Draft AI Basic Act.

- **Data Governance:** While Article 14 of the Draft AI Basic Act promotes the establishment of mechanisms for data governance, including details of evaluation of training data, feedback mechanism, etc., the Draft AI Basic Act fails to elaborate on the details. Furthermore, the Draft AI Basic Act has not established a mechanism of impact assessment for AI mentioned in Paragraph 72 of the UNESCO Recommendation.

- **Data Transparency:** The principle of transparency listed in Item 5, Article 3 of the Draft AI Basic Act is aligned with Paragraph 73 of the UNESCO Recommendation. But the data subjects' rights and the ability to access and erase their personal data in AI systems are not specified in the Draft AI Basic Act.

- **Open Data and Data Sharing:** Article 15 of the Draft AI Basic Act is consistent with the requirement of open data in Paragraph 75 of the UNESCO Recommendation. However, unlike Paragraphs 76 and 77 of the UNESCO Recommendation, the Draft AI Basic Act does not explicitly mention the authority's obligation to establish gold standard datasets or collaborative platforms with private efforts.

REUTERS/Romeo Ranoco

Conclusion

As AI becomes increasingly central to decision-making processes across governments, industries and other sectors, the need for responsible, ethical, and human-centered data use has never been more critical. Responsible data use in AI is crucial to ensure that systems are fair, transparent, and respect human rights, minimizing harm and fostering trust in their outcomes.

We have observed that AI governance frameworks can take many forms (ranging from comprehensive laws and binding regulations to soft law instruments like guidelines, strategies, and codes of practice) each offering different pathways to promote responsible data use. This report reveals that while many countries are actively developing AI strategies and legal frameworks, there is still uneven progress in embedding robust data governance principles into those efforts.

Key challenges in the studied jurisdictions include the lack of AI-specific legal provisions, insufficient attention to sensitive data like biometrics, and limited mechanisms for transparency and accountability in automated decision-making. Current data regulations provide important safeguards for individuals' personal data, but they are not sufficient for addressing all the regulatory issues associated with data in AI systems. In addition to the above-mentioned challenges, other regulatory gaps where these regulations fall short include use of synthetic data; explainability of AI decisions; sector-specific risks (e.g. healthcare); data provenance and consenting in training, among other possible examples.

Encouragingly, many of the jurisdictions studied are drawing on internationally recognized principles, such as those outlined by the OECD and UNESCO, to shape their AI and data governance landscapes. These global benchmarks provide a strong foundation for building interoperable, rights-based frameworks that can both foster innovation and safeguard public trust. To fully realize the benefits of AI while minimizing its risks, countries are moving from guidelines to enforceable standards, ensuring that legal and institutional frameworks are equipped to handle the complexities of AI systems.
The research reveals a core set of shared principles that are increasingly reflected in national AI frameworks. These include transparency, accountability, data protection, human oversight, and fairness, each essential to building trustworthy AI systems.

We have also observed that transparency and accountability in data use are critical to ensuring that AI systems can be audited, challenged, and trusted, especially when they impact people's rights, opportunities, and access to services, while strong data protection is fundamental as it safeguards individuals' privacy, prevents misuse of sensitive information, and reinforces public confidence in the ethical use of technology. In addition, in order to ensure effective implementation of responsible data use in AI, it is essential that enforcement authorities (such as data protection agencies and sectoral regulators) are empowered with clear mandates, adequate resources, and cross-sectoral coordination mechanisms.

This study also highlights the importance of international collaboration, cross-sectoral dialogue, and ongoing legal reform (e.g. integrating and taking into account in legislative processes principles such as those mentioned by the OECD and UNESCO, participating in multi-stakeholder dialogues that work to translate technical principles into frameworks, actively participating in forums, etc). Strengthening the connection between AI strategies and data regulations is essential to creating AI ecosystems that are not only technically robust but also socially responsible.

We hope this work serves as a valuable tool for stakeholders working to advance fair, inclusive, and rights-respecting AI governance worldwide.

The Thomson Reuters Foundation's global pro bono legal network, TrustLaw, works with leading law firms and corporate legal teams to facilitate free legal support, research, and resources for civil society organizations, social enterprises, and non-profit independent media around the globe.

For more information, visit www.trust.org.

TrustLaw | Thomson Reuters Foundation