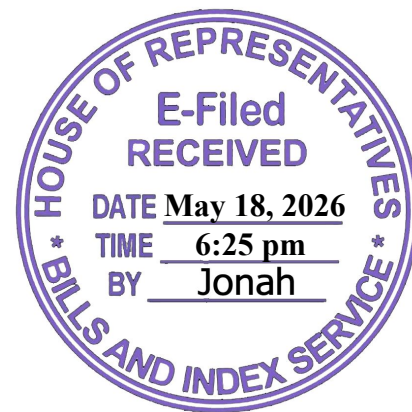


Republic of the Philippines
HOUSE OF REPRESENTATIVES
Constitution Hills, Quezon City

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 9304



Introduced by Lone District of Agusan del Norte Representative
HON. DALE B. CORVERA

AN ACT
ESTABLISHING A NATIONAL FRAMEWORK FOR TRUSTWORTHY
ARTIFICIAL INTELLIGENCE IN THE PHILIPPINES, PROVIDING FOR
RISK-BASED REGULATION, SAFETY STANDARDS, AND PUBLIC
ACCOUNTABILITY, AND CREATING THE BUREAU OF ARTIFICIAL
INTELLIGENCE SYSTEMS

EXPLANATORY NOTE

Artificial Intelligence (AI) is rapidly transforming economies, governance, and everyday life. It is projected to contribute up to US\$15.7 trillion to the global economy by 2030, underscoring its potential as a driver of productivity and innovation.¹ However, alongside these opportunities are significant risks, including algorithmic bias, data privacy violations, lack of transparency, and the erosion of human accountability in decision-making.²

Globally, governments have begun establishing frameworks to ensure that AI systems are deployed in a manner that is ethical, safe, and aligned with public interest. The Organisation for Economic Co-operation and Development has adopted principles emphasizing transparency, accountability, and human-centered values in AI systems.³ Similarly, the United Nations Educational, Scientific and Cultural Organization has issued a Recommendation on the Ethics of Artificial Intelligence, calling for safeguards that protect human rights, promote fairness, and ensure inclusivity in AI deployment.⁴ The European Union, through its AI regulatory framework, has also introduced a risk-based approach to governance, particularly regulating high-risk AI systems in critical sectors.⁵

In the Philippines, while the Republic Act No. 10173 provides safeguards for personal data, there remains no comprehensive legal framework governing the broader design, deployment, and accountability of AI systems. As AI becomes increasingly embedded in sectors such as healthcare, finance, education, governance, and public safety, the absence of a unified regulatory structure exposes individuals and institutions to risks that current laws do not fully address.

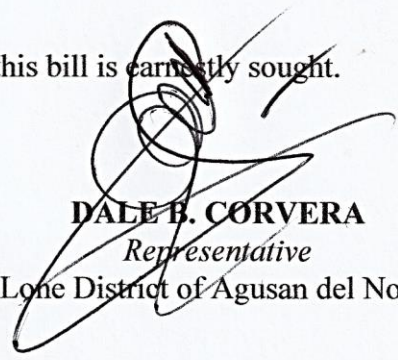
This bill seeks to establish the AI Governance Act of the Philippines, creating a comprehensive governance framework that ensures AI systems are developed and deployed in a manner that is ethical, secure, transparent, and inclusive. It proposes the creation of a dedicated regulatory

body, the Bureau of Artificial Intelligence Systems (BAIS), to oversee compliance, enforce standards, and guide national AI development.

The measure adopts a risk-based regulatory approach, requiring stricter oversight for high-risk AI systems while allowing innovation to flourish through regulatory sandboxes and adaptive governance mechanisms. It establishes a Bill of Rights in Artificial Intelligence to protect individuals from harmful algorithmic outcomes, ensures meaningful human oversight in critical decisions, and mandates transparency, accountability, and fairness in AI deployment.

Ultimately, this measure aims to position the Philippines as a responsible and competitive participant in the global AI ecosystem, fostering innovation while safeguarding fundamental rights, democratic values, and public trust.

In view of the foregoing, the immediate passage of this bill is earnestly sought.



DALE B. CORVERA
Representative
Lone District of Agusan del Norte

1. PricewaterhouseCoopers, *Sizing the Prize: What's the Real Value of AI for Your Business and How Can You Capitalise* (2017).

2. National Institute of Standards and Technology, *AI Risk Management Framework 1.0* (2023).

3. Organisation for Economic Co-operation and Development, *OECD Principles on Artificial Intelligence* (2019).

4. United Nations Educational, Scientific and Cultural Organization, *Recommendation on the Ethics of Artificial Intelligence* (2021).

5. European Union Artificial Intelligence Act (2024).

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Constitution Hills, Quezon City

TWENTIETH CONGRESS
First Regular Session

HOUSE BILL NO. 9304

Introduced by Lone District of Agusan del Norte Representative
HON. DALE B. CORVERA

AN ACT
ESTABLISHING A NATIONAL FRAMEWORK FOR TRUSTWORTHY
ARTIFICIAL INTELLIGENCE IN THE PHILIPPINES, PROVIDING FOR
RISK-BASED REGULATION, SAFETY STANDARDS, AND PUBLIC
ACCOUNTABILITY, AND CREATING THE BUREAU OF ARTIFICIAL
INTELLIGENCE SYSTEMS

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

CHAPTER I
GENERAL PROVISIONS

SECTION 1. Title. This Act shall be known as the “*AI Governance Act of the Philippines.*”

SEC. 2. Declaration of Policy. It is the policy of the State to promote the ethical, secure, and inclusive development, deployment, and use of Artificial Intelligence (AI) in a manner that strengthens national innovation, protects fundamental rights, preserves human dignity, and advances the public good.

The State shall ensure that AI technologies deployed in the Philippines are human-centric, trustworthy, accountable, transparent, and aligned with constitutional principles, democratic values, and the rule of law.

The State shall establish a comprehensive governance framework that enables the responsible development and deployment of AI systems while safeguarding individuals, communities, and institutions from potential harms arising from misuse, abuse, or unintended consequences of such technologies.

The State shall ensure that an appropriate legal basis is established for the processing of personal data by AI systems, in full alignment with existing laws on data privacy, cybersecurity, and human rights.

The State shall guarantee user transparency. Individuals shall be informed, in a clear and accessible manner, when they are interacting with an AI system, unless such interaction is clearly evident from the context and circumstances. Individuals shall likewise be notified whenever their personal data will be collected, processed, or utilized by such systems.

Where an AI system utilizes personal data for decision-making, including profiling or automated evaluation, the State shall ensure that the user is informed of the existence of such processing, the logic involved, and the potential consequences of such decisions.

Privacy risk assessments shall be conducted prior to the implementation of AI systems, and commensurate data protection and security measures shall be adopted in accordance with the level of risk posed to individuals.

The principles of data minimization, purpose limitation, proportionality, and accuracy shall be strictly observed in all AI systems.

Certain AI systems shall not be permitted to process personal data or generate outputs where such processing poses unacceptable risks to individuals, particularly in cases involving exploitation of vulnerable groups or threats to health, safety, or fundamental rights.

The use of real-time biometric identification systems, as well as the processing of sensitive personal data, shall be undertaken only with strict safeguards, lawful basis, and regulatory oversight.

In the case of generative AI systems, safeguards shall be implemented to ensure that outputs do not reveal, reconstruct, or infer personal or sensitive data of individuals without lawful basis or consent.

The State shall adopt specific protections for minors and vulnerable sectors, ensuring that AI systems are designed and deployed in a manner that upholds their rights, safety, dignity, and welfare.

The State shall promote innovation while ensuring that such innovation does not compromise human dignity, democratic accountability, or social justice.

SEC. 3. Scope and Coverage. This Act shall apply to the research, design, development, training, testing, validation, deployment, use, importation, distribution, sale, and regulation of Artificial Intelligence systems across all sectors within the jurisdiction of the Republic of the Philippines.

It shall govern both public and private entities engaged in AI-related activities, including natural and juridical persons, government agencies, government-owned or controlled corporations, educational institutions, and foreign entities operating within or affecting Philippine territory.

This Act shall likewise apply to AI systems deployed outside the Philippines where such systems produce effects on individuals, institutions, or markets within the Philippines, including cross-border digital platforms, online services, and remote processing systems.

The provisions of this Act shall apply regardless of whether the AI system is developed domestically or internationally, provided that its outputs, decisions, or impacts affect persons or entities within Philippine jurisdiction.

SEC. 4. Definition of Terms. For purposes of this Act, the following terms are defined:

(a) *Artificial Intelligence (AI)* refers to any artificial or engineered system, whether embodied in hardware, software, or integrated into digital platforms, that is designed to perform tasks requiring human-like perception, cognition, reasoning, learning, decision-making, communication, or physical action, with varying levels of autonomy;

(b) *AI System* means a machine-based system that, for explicit or implicit objectives, processes input data to generate outputs such as predictions, classifications, recommendations, content, or decisions that influence physical or virtual environments;

(c) *High-risk AI System* refers to an AI system that, by virtue of its function, deployment context, or scope, poses a significant risk to the rights, safety, security, economic interests, or welfare of individuals or the public;

(d) *Autonomous AI System* refers to an AI system that, once activated, can operate independently of real-time human control or continuous supervision and may adapt or modify its behavior within a defined operational scope;

(e) *Training Data* refers to any dataset used to train, validate, or fine-tune an AI model, whether labeled or unlabeled, structured or unstructured, synthetic or real;

(f) *Model* refers to a mathematical, statistical, or computational representation trained on data that enables an AI system to generate outputs based on learned patterns;

(g) *Foundation Model* refers to a large-scale AI model trained on broad datasets and capable of being adapted to a wide range of downstream tasks through fine-tuning or prompting;

(h) *Generative AI* refers to AI systems capable of autonomously producing content such as text, images, audio, video, code, or synthetic data that resembles or simulates human-generated outputs;

(i) *Algorithmic Transparency* refers to the degree to which the logic, structure, assumptions, data inputs, and decision pathways of an AI system can be meaningfully understood, explained, and communicated;

(j) *Human Oversight* refers to the presence of operational procedures and technical mechanisms that allow humans to monitor, understand, intervene in, suspend, or override the functioning of an AI system;

(k) *Deployment* refers to the act of making an AI system operational in any environment where its outputs may influence decisions, actions, or outcomes;

(l) *Bureau of Artificial Intelligence Systems (BAIS)* refers to the regulatory body created under this Act;

(m) *Internal AI Compliance Unit (IACU)* refers to an internal body within an organization responsible for ensuring compliance with this Act;

(n) *Code of AI Regulations (CAIR)* refers to the official compendium of rules, standards, and guidelines issued pursuant to this Act;

(o) *Regulatory Sandbox* refers to a controlled, supervised, and time-bound environment that allows testing of AI systems under regulatory oversight;

(p) *Explainability* refers to the capability of an AI system to provide understandable and interpretable reasons for its outputs;

(q) *Social Scoring* refers to the evaluation or ranking of individuals based on aggregated personal data or behavior;

(r) *Synthetic Content* refers to media or outputs generated or altered by AI that simulate real or fictional entities;

(s) *Incident Report* refers to a formal submission documenting adverse events or failures involving an AI system;

(t) *Profiling* refers to automated processing of personal data to evaluate or predict aspects of an individual;

(u) *Public-sector AI* refers to AI systems used by government entities;

(v) *Adverse Algorithmic Outcome* refers to materially harmful decisions or outputs affecting individuals;

(w) *Digital Dignity* refers to the principle that individuals interacting with AI systems retain their autonomy, respect, and human status;

(x) *Bias Testing* refers to the systematic evaluation of AI systems to identify and mitigate discriminatory outcomes.

CHAPTER II

BILL OF RIGHTS IN ARTIFICIAL INTELLIGENCE AND GOVERNANCE

SEC. 5. Bill of Rights in Artificial Intelligence. In recognition of the transformative impact of Artificial Intelligence on human life, work, governance, and society, and in order to preserve human dignity, democratic accountability, social justice, and the public good, the State hereby affirms and guarantees the following rights of all persons within its jurisdiction in relation to the design, development, deployment, and use of Artificial Intelligence systems:

(a) *Right to Meaningful Human Oversight.* All persons shall have the right to meaningful human oversight in decisions that affect their rights, freedoms, opportunities, safety, or access to essential services. No AI system shall be granted final authority over decisions that produce legal, material, or similarly significant effects on individuals without the availability of a mechanism for timely human review, intervention, correction, or override by a competent and accountable human authority. Human oversight shall not be merely symbolic or perfunctory, but shall be designed to ensure actual control, understanding, and responsibility over the outputs and consequences of AI systems.

(b) *Right to Transparency and Awareness.* All persons shall have the right to know when they are interacting with, subject to, or affected by an Artificial Intelligence system. Entities deploying AI systems shall provide clear, accessible, and timely disclosure regarding:

1. The use of AI in the interaction, service, or decision-making process;
2. The general purpose, function, and capabilities of the AI system;
3. The extent to which the AI system contributes to or determines outcomes affecting the individual; and
4. The existence of automated processing, including profiling or classification where applicable.

Such disclosures shall be presented in a manner that is understandable to the average user and appropriate to the context of use.

(c) *Right to Explanation and Interpretability.* All persons shall have the right to obtain a meaningful explanation of decisions, recommendations, or outputs generated by AI systems that affect them. Such explanation shall include, to the extent practicable:

1. The basis or rationale of the decision;
2. The key factors or inputs that influenced the outcome; and
3. The general logic or methodology used by the system.

The level of explanation required shall be proportionate to the risk, impact, and complexity of the AI system.

(d) *Right to Non-Discrimination and Fair Treatment.* All persons shall have the right to be protected from algorithmic discrimination, bias, or unfair treatment arising from the use of Artificial Intelligence systems. AI systems shall not produce outcomes that result in unjust or disproportionate discrimination on the basis of race, ethnicity, gender, sex, religion, age, disability, socioeconomic status, geographic location, political beliefs, or any other protected characteristic. Entities deploying AI systems shall take

reasonable and proactive measures to identify, test, mitigate, and monitor biases in datasets, models, and outputs.

(e) *Right to Privacy and Data Protection.* All persons shall retain meaningful control over their personal data used in Artificial Intelligence systems. This shall include the right to:

1. Be informed of the collection and processing of personal data;
2. Access and obtain a copy of their personal data;
3. Correct inaccurate or incomplete data;
4. Object to or restrict certain forms of processing; and
5. Request deletion or erasure of personal data, subject to applicable law.

AI systems shall be designed and implemented in accordance with the principles of data minimization, purpose limitation, proportionality, security, and accountability.

(f) *Right to Safety and Protection from Harm.* All persons shall be protected from unsafe, unreliable, or harmful Artificial Intelligence systems. High-risk AI systems shall be subject to:

1. Pre-deployment review and certification;
2. Continuous monitoring and auditing;
3. Risk mitigation and fail-safe mechanisms; and
4. Clearly identified accountability structures.

No AI system shall be deployed where it poses an unacceptable risk to health, safety, or fundamental rights.

(g) *Right to Redress and Remedy.* All persons adversely affected by an AI system shall have the right to seek redress. This shall include:

1. The right to request human intervention, review, or reconsideration of an AI-generated decision;
2. The right to obtain correction of erroneous or harmful outputs;
3. Access to administrative, civil, or judicial remedies; and
4. The right to compensation for damages where appropriate.

Entities deploying AI systems shall establish accessible and effective mechanisms for complaints, appeals, and dispute resolution.

(h) *Right to the Protection of Labor and Human Dignity.* The dignity of labor and human capability shall be preserved in the age of Artificial Intelligence. Workers affected by automation, augmentation, or displacement due to AI shall be entitled to:

1. Just transition mechanisms;
2. Reskilling and upskilling opportunities;
3. Protection against unfair labor practices; and
4. Access to new employment opportunities.

AI systems shall not be used to undermine fundamental labor rights, including the right to fair wages, safe working conditions, and collective organization.

(i) *Right to Participation and Democratic Governance.* All persons shall have the right to be informed of, participate in, and contribute to the development of policies governing Artificial Intelligence. The State shall ensure public consultation, transparency, and access to information in the formulation of AI-related laws, regulations, and standards. Mechanisms shall be established to allow civil society, academia, industry, and affected communities to participate meaningfully in AI governance.

Nothing in this Chapter shall be construed to limit, diminish, or supersede any rights or protections guaranteed under the Constitution, the Data Privacy Act of 2012, or other applicable laws. The rights enumerated herein shall be interpreted in a manner that promotes human dignity, equality, justice, and the responsible advancement of technology.

CHAPTER III

GOVERNANCE FRAMEWORK FOR ARTIFICIAL INTELLIGENCE

SEC. 6. Creation of the Bureau of Artificial Intelligence Systems (BAIS). There is hereby created a Bureau of Artificial Intelligence Systems (BAIS) under the Department of Information and Communications Technology (DICT).

The BAIS shall serve as the central regulatory, technical, investigatory, administrative, and enforcement body of the State on all matters relating to the governance, oversight, and regulation of Artificial Intelligence systems in the Philippines.

The BAIS shall operate under the direct supervision and control of the Secretary of Information and Communications Technology, who shall exercise authority over its strategic direction, regulatory priorities, and administrative oversight. All decisions, issuances, and enforcement actions of the BAIS shall be subject to the policy guidance and institutional coordination of the DICT. The DICT shall ensure that the BAIS is adequately funded, properly staffed, and fully integrated into the national digital governance infrastructure.

The Secretary of the DICT shall exercise final authority in resolving jurisdictional questions involving the BAIS and other bureaus or offices within the Department and may issue such directives as may be necessary to ensure coherence, consistency, and effectiveness in national digital and AI policy.

SEC. 6-A. National Artificial Intelligence Strategy. The Department of Information and Communications Technology, through the BAIS, in coordination with the Department of Economy, Planning, and Development (DEPDev), the Department of Science and Technology (DOST), and other relevant government agencies, shall develop, adopt, and periodically update a National Artificial Intelligence Strategy. The National Artificial Intelligence Strategy shall:

- a) Identify priority sectors for AI development and deployment, including but not limited to healthcare, education, agriculture, finance, governance, public safety, climate resilience, and disaster risk reduction;
- b) Promote the development of a competitive, inclusive, and innovation-driven domestic AI ecosystem, including startups, micro, small, and medium enterprises (MSMEs), academic institutions, and research organizations;
- c) Align AI development with national economic goals, labor policies, educational systems, digital infrastructure planning, and industrial development strategies;
- d) Establish measurable targets, benchmarks, and timelines for AI adoption, innovation, and integration into public and private sector operations;
- e) Ensure equitable access to AI technologies across geographic regions, sectors, and socioeconomic groups, including underserved and marginalized communities;
- f) Promote ethical, safe, and responsible AI innovation in accordance with the principles established under this Act;

- g) Provide mechanisms for monitoring, evaluation, and periodic review of AI development, including performance indicators and accountability measures; and
- h) Integrate AI policy into the Philippine Development Plan and other national planning frameworks.

SEC. 7. Mandate and Powers of the Bureau. The BAIS shall have the following powers and functions:

- a) Formulate, issue, and enforce rules, standards, protocols, and technical requirements governing the design, development, training, testing, deployment, use, importation, and regulation of Artificial Intelligence systems;
- b) Classify AI systems according to levels of risk, sensitivity, autonomy, and potential impact, and determine which systems shall be designated as high-risk, limited-risk, or minimal-risk;
- c) Maintain and administer a National Registry of Artificial Intelligence Systems, and require all entities deploying or operating AI systems to comply with registration, reporting, and documentation requirements;
- d) Conduct pre-deployment reviews, risk assessments, technical evaluations, and certification processes for high-risk AI systems prior to their deployment or use;
- e) Conduct periodic audits, inspections, and post-deployment monitoring of AI systems to ensure continued compliance with this Act and applicable regulations;
- f) Issue permits, certifications, licenses, or approvals for the development, testing, and deployment of AI systems, subject to compliance with regulatory requirements;
- g) Issue cease-and-desist orders, suspension orders, or prohibition orders against AI systems that pose significant risks to public safety, national security, or individual rights;
- h) Exercise visitorial powers, including the authority to inspect premises, examine records, require the submission of documents, and access technical logs and system documentation necessary for compliance verification;
- i) Initiate investigations, administrative proceedings, and enforcement actions against entities found to be in violation of this Act;
- j) Refer cases involving criminal violations to the Department of Justice and coordinate with law enforcement agencies for prosecution;
- k) Issue binding advisory opinions, interpretive guidelines, and regulatory clarifications on matters relating to AI governance;
- l) Establish, maintain, and update the Code of Artificial Intelligence Regulations (CAIR), which shall serve as the official compendium of all implementing rules, technical standards, compliance procedures, and regulatory issuances under this Act;
- m) Promote the development of domestic AI capabilities, including research, innovation, infrastructure, and talent development, consistent with ethical and human-centered standards;
- n) Develop and implement national programs on AI safety, risk mitigation, accountability, and public awareness;

- o) Establish regulatory sandbox programs and innovation testbeds in accordance with this Act; and
- p) Perform such other functions as may be necessary or incidental to carry out the provisions of this Act.

SEC. 8. Organizational Structure of the Bureau. The BAIS shall be headed by a Director, who shall be appointed by the President of the Philippines, upon the recommendation of the Secretary of Information and Communications Technology. The Bureau shall be composed of the following divisions:

- a) Standards and Safety Division – responsible for risk classification, certification, testing protocols, and safety evaluations of AI systems;
- b) Ethics and Oversight Division – responsible for ensuring compliance with ethical principles, human oversight requirements, and accountability mechanisms;
- c) Compliance and Sectoral Integration Division – responsible for coordinating with public agencies, private sector entities, and regulated industries to ensure alignment with this Act;
- d) Infrastructure and Research Division – responsible for supporting national AI infrastructure, research initiatives, open-source development, and regulatory sandbox programs; and
- e) Investigations and Enforcement Division – responsible for investigating violations, conducting enforcement actions, and recommending sanctions.

The BAIS may create additional units, technical committees, or advisory bodies as may be necessary for the effective implementation of its mandate.

SEC. 9. Rule-Making Authority and the Code of Artificial Intelligence Regulations (CAIR). The BAIS shall promulgate such rules, regulations, and technical standards as may be necessary to implement the provisions of this Act.

All such rules, standards, procedures, and interpretive guidance shall be compiled into a unified compendium known as the Code of Artificial Intelligence Regulations (CAIR). The CAIR shall:

- a. Serve as the official and authoritative repository of all enforceable regulatory issuances relating to AI;
- b. Be made publicly accessible through official government platforms;
- c. Be regularly updated to reflect technological developments, emerging risks, and regulatory best practices; and
- d. Provide clear, practical guidance to regulated entities on compliance obligations.

SEC. 10. Consultation and Publication Requirements. The BAIS shall ensure that all proposed regulations, standards, and issuances are subject to public notice and consultation. Such consultation shall be conducted for a period of not less than fifteen (15) calendar days; include participation from relevant stakeholders, including government agencies, private sector entities, academic institutions, civil society organizations, and technical experts; and be conducted in a transparent and accessible manner.

All final rules and regulations shall be published in the Official Gazette or in a newspaper of general circulation; and posted on the official website of the DICT and the BAIS.

SEC. 11. Internal AI Compliance Units (IACUs). All public agencies, government-owned or controlled corporations, and regulated private entities that develop, deploy, or operate Artificial Intelligence systems shall establish an Internal AI Compliance Unit (IACU). The IACU shall be responsible for:

- a. Ensuring internal compliance with this Act and all applicable regulations;
- b. Developing and implementing internal AI governance frameworks, risk management systems, and compliance protocols;
- c. Conducting internal audits, bias testing, safety evaluations, and performance monitoring of AI systems;
- d. Maintaining comprehensive documentation of AI system design, training data, model architecture, deployment context, and operational performance;
- e. Preparing and submitting required reports, disclosures, and documentation to the BAIS;
- f. Coordinating with the BAIS during inspections, audits, and investigations; and
- g. Immediately suspending, escalating, or reporting any AI system that poses an imminent risk to individuals, public safety, or institutional integrity.

The BAIS may deputize IACUs to perform specific compliance and monitoring functions under its supervision.

SEC. 12. Annual Report to Congress. The BAIS shall submit an annual report to Congress, through the appropriate committees of the House of Representatives and the Senate, detailing:

- a. The status of AI development, deployment, and adoption in the Philippines;
- b. The number, classification, and characteristics of AI systems registered, including high-risk systems;
- c. Enforcement actions taken, including investigations, sanctions, and compliance measures;
- d. Emerging risks, technological trends, and policy challenges;
- e. The impact of AI on employment, economic development, public services, and social welfare; and
- f. Recommendations for legislative, regulatory, or policy reforms.

The report shall be made publicly available, subject to confidentiality and national security considerations.

CHAPTER IV

ETHICAL AND LEGAL STANDARDS FOR ARTIFICIAL INTELLIGENCE SYSTEMS

SEC. 13. Principles of Ethical Artificial Intelligence. All Artificial Intelligence systems developed, designed, trained, tested, deployed, imported, or used within the jurisdiction of the Republic of the Philippines shall adhere to the following core principles:

- a. **Respect for Human Dignity and Rights.** – AI systems shall be designed, developed, and deployed in a manner that respects the inherent dignity, autonomy, and fundamental rights of all persons;
- b. **Fairness and Non-Discrimination.** – AI systems shall not result in unjust or disproportionate discrimination based on race, ethnicity, gender, sex, religion, age, disability, socioeconomic status, political beliefs, geographic location, or any other protected characteristic;
- c. **Data Privacy and Protection.** – AI systems shall comply with the Data Privacy Act of 2012 and all applicable laws on personal data protection, and shall ensure lawful, fair, and transparent processing of data;
- d. **Robustness, Safety, and Security.** – AI systems shall be developed and tested to ensure resilience against errors, manipulation, cyberattacks, and unintended consequences;

- e. Accountability. – Clear lines of responsibility shall be established for the design, deployment, and outcomes of AI systems, ensuring that accountable human actors remain responsible for system behavior;
- f. Transparency and Explainability. – AI systems shall be sufficiently transparent and explainable, particularly in high-risk contexts, to allow meaningful understanding of outputs and decisions;
- g. Proportionality and Risk-Based Regulation. – AI systems shall be regulated in a manner commensurate with their level of risk, scale of deployment, and potential impact on individuals and society; and
- h. Human-Centered Design. – AI systems shall prioritize human well-being, safety, and agency in all stages of development and deployment.

SEC. 14. Classification of High-Risk Artificial Intelligence Systems. The BAIS shall classify certain Artificial Intelligence systems as high-risk based on their function, deployment context, and potential to cause harm. An AI system shall be considered high-risk where it involves any of the following:

- a. Potential to affect fundamental rights, civil liberties, or access to essential services;
- b. Use in critical sectors such as healthcare, finance, education, employment, law enforcement, public safety, or government decision-making;
- c. Degree of autonomy, particularly where there is limited or no meaningful human oversight;
- d. Use for profiling, surveillance, biometric identification, behavioral prediction, or predictive policing;
- e. Scale and scope of deployment affecting large populations or critical infrastructure;
- f. Potential to produce irreversible, systemic, or widespread harm; or
- g. Any other criteria as may be determined by the BAIS through regulation.

High-risk AI systems shall be subject to mandatory registration, pre-deployment review, certification, risk mitigation requirements, and continuous monitoring under this Act.

SEC. 15. Disclosure Obligations. Any person or entity deploying an Artificial Intelligence system shall be under obligation to disclose, in a clear, conspicuous, and timely manner, the following information to affected individuals:

- a. That the interaction, service, or decision involves the use of an AI system;
- b. The general purpose, scope, and intended function of the AI system;
- c. Whether and to what extent the AI system is capable of making or contributing to automated decisions that may affect the rights, interests, or obligations of individuals;
- d. The nature of the data being processed, including whether personal or sensitive personal data is involved;
- e. The existence of profiling, automated evaluation, or decision-making processes, where applicable; and

- f. The accessible channels or mechanisms available for appeal, correction, human review, or redress.

Such disclosures shall be made in plain, understandable language appropriate to the context and user group.

SEC. 16. Consent, Lawful Processing, and Data Ethics. No Artificial Intelligence system shall be trained, tested, validated, or deployed using personal data obtained without a lawful basis or informed consent, where required under applicable law. Data used in AI systems shall:

- a. Be relevant, necessary, and proportionate to the intended purpose;
- b. Be accurate, complete, and kept up to date;
- c. Be processed in accordance with principles of transparency, fairness, and accountability; and
- d. Be anonymized or pseudonymized, where feasible and appropriate.

The use of sensitive personal data shall be subject to heightened safeguards, strict access controls, and regulatory oversight. Entities shall implement data governance frameworks that ensure responsible data sourcing, labeling, storage, and use throughout the lifecycle of the AI system.

SEC. 17. Transparency, Documentation, and Accountability Requirements. All high-risk Artificial Intelligence systems shall be accompanied by comprehensive documentation sufficient to enable regulatory oversight, auditing, and accountability. Such documentation shall include, but not be limited to:

- a. A detailed description of the AI system, including its purpose, functionality, and intended use cases;
- b. Information on the model architecture, design choices, and training methodologies;
- c. Documentation of datasets used, including sources, characteristics, limitations, and potential biases;
- d. Evidence of testing, validation, and evaluation procedures, including bias testing and performance benchmarking;
- e. Description of risk mitigation measures and safeguards implemented;
- f. Explanation of decision-making pathways or output generation processes, where applicable;
- g. Records of system performance, monitoring results, and updates post-deployment; and
- h. Mechanisms for human oversight, intervention, and system override.

The BAIS may prescribe additional technical documentation requirements under the CAIR.

SEC. 18. Prohibited Practices. The following uses of Artificial Intelligence systems are hereby strictly prohibited:

- a. The use of AI systems to intentionally deceive, manipulate, or mislead individuals without clear disclosure, particularly in political, financial, or public interest contexts;
- b. The deployment of autonomous AI systems in contexts involving life, liberty, or fundamental rights where there is no effective mechanism for meaningful human intervention, including but not limited to lethal force applications;

- c. The use of AI systems for the purpose of exploiting vulnerable populations, including children, persons with disabilities, the elderly, or economically disadvantaged individuals, through manipulative design, coercive targeting, or deceptive practices;
- d. The use of AI systems for unlawful surveillance, mass profiling, or social control in a manner that violates constitutional rights or due process;
- e. The use of AI systems for unauthorized biometric identification or real-time tracking of individuals in public or private spaces, except as expressly authorized by law and subject to strict safeguards;
- f. The deployment of AI systems that generate or disseminate synthetic content for the purpose of impersonation, fraud, or disinformation without proper disclosure and consent; and
- g. Any other use of AI systems that the BAIS may determine, through regulation, to pose unacceptable risks to individuals, public safety, national security, or democratic institutions.

Violations of this Section shall be subject to the penalties and sanctions provided under this Act and other applicable laws.

CHAPTER V

SECTOR-SPECIFIC RULES AND OBLIGATIONS

SEC. 19. Artificial Intelligence in Government Services. Government agencies, instrumentalities, government-owned or controlled corporations, and local government units that develop, procure, or deploy Artificial Intelligence systems for administrative, operational, regulatory, or public-facing functions shall comply with the following:

- a. All AI systems shall be registered with the BAIS prior to deployment, including submission of required documentation, risk classification, and intended use;
- b. AI-generated outputs shall remain subject to human validation, supervision, and legal accountability, and shall not replace the exercise of statutory or constitutional duties of public officials;
- c. A clear and publicly accessible statement describing the function, purpose, scope, limitations, and appeal mechanisms of the AI system shall be published on official platforms;
- d. Agencies shall maintain comprehensive audit logs, decision records, and documentation of AI-assisted processes to ensure traceability and accountability;
- e. No AI system shall be used to render final determinations affecting rights, obligations, or entitlements without meaningful human review;
- f. Agencies shall ensure that AI systems comply with standards of transparency, fairness, accessibility, and non-discrimination;
- g. Agencies shall implement data protection, cybersecurity, and system integrity measures appropriate to the level of risk.

The BAIS may grant limited exemptions for internal-use tools or sandbox deployments, provided that risks are minimal, documented, and subject to oversight.

SEC. 20. Artificial Intelligence in Education. Artificial Intelligence systems used in educational institutions, whether public or private, shall comply with the following:

- a. AI systems shall support and enhance, and not replace, the role of human educators;
- b. AI shall not be used as the sole basis for determining official grading, ranking, academic evaluation, or disciplinary action;

- c. Students, parents, and educators shall be informed of the use of AI systems, including their purpose, limitations, and impact;
- d. AI-generated outputs shall be explainable, accessible, and subject to human review;
- e. Educational institutions shall ensure that AI systems do not reinforce bias, discrimination, or inequitable learning outcomes;
- f. Schools shall adopt internal governance policies on AI use, including ethical standards and safeguards for minors.

The BAIS shall coordinate with the Department of Education (DepEd) and the Commission on Higher Education (CHED) in issuing sector-specific guidelines.

SEC. 21. Artificial Intelligence in Healthcare and Medical Decision-Making. No Artificial Intelligence system shall be deployed for diagnostic, triage, treatment, or clinical prioritization purposes unless the following conditions are met:

- a. Review, evaluation, and certification by the Department of Health (DOH), in coordination with the BAIS;
- b. Continuous human oversight by a duly licensed medical professional, with AI outputs deemed assistive and non-determinative;
- c. Full disclosure to patients regarding the role, capabilities, and limitations of the AI system;
- d. Maintenance of clinical accountability by licensed healthcare providers;
- e. Compliance with applicable medical, ethical, and data protection standards;
- f. Implementation of risk management, validation, and performance monitoring protocols.

The BAIS may authorize provisional deployment of emerging AI systems under a regulatory sandbox framework for controlled clinical testing, subject to strict safeguards and reporting requirements.

SEC. 22. Artificial Intelligence in Finance, Insurance, and Credit Risk Modeling. Financial institutions, insurance entities, cooperatives, and other regulated financial actors using AI systems shall comply with the following:

- a. Disclosure of the use of AI in pricing, underwriting, credit scoring, risk assessment, or policy decisions;
- b. Conduct and retention of bias testing, fairness assessments, and validation reports for regulatory review;
- c. Establishment of mechanisms for human intervention, review, or override of AI-generated decisions;
- d. Provision of accessible appeal processes for affected individuals;
- e. Submission of high-risk AI systems for registration and classification with the BAIS;
- f. Compliance with sectoral regulations issued by the Bangko Sentral ng Pilipinas (BSP), Securities and Exchange Commission (SEC), Insurance Commission, and Cooperative Development Authority (CDA).

The BAIS may adopt differentiated compliance requirements for low-risk or low-volume applications.

SEC. 23. Artificial Intelligence in Employment and Human Resources. Employers and organizations using AI systems for recruitment, evaluation, promotion, discipline, or termination shall:

- a. Inform applicants and employees of the use of AI systems in employment-related decisions;
- b. Conduct fairness, bias, and impact assessments;
- c. Ensure that no employment decision is based solely on AI outputs;
- d. Provide mechanisms for human review, appeal, and correction;

- e. Maintain documentation of AI systems for regulatory inspection;
- f. Protect workers from discriminatory, invasive, or unjust automated practices.

Microenterprises and small businesses may be subject to simplified compliance standards as may be determined by the BAIS in coordination with DOLE.

SEC. 24. Artificial Intelligence in Law Enforcement, Security, and Surveillance. AI systems used for law enforcement, surveillance, profiling, or public safety shall be classified as high-risk and shall be subject to the following:

- a. Prior written authorization from the Secretary of the Interior and Local Government, with review by the BAIS;
- b. Strict prohibition of indiscriminate, real-time mass surveillance unless expressly authorized by law and subject to judicial oversight;
- c. Continuous human control over all AI-assisted decisions;
- d. Independent post-deployment audits and evaluation;
- e. Transparency and public notice where feasible, consistent with national security considerations;
- f. Safeguards to ensure compliance with constitutional rights, due process, and human rights standards.

SEC. 25. Artificial Intelligence in Critical Infrastructure and Public Utilities.

Operators of critical infrastructure, including but not limited to energy, water, telecommunications, transportation, and financial systems, shall:

- a. Report all AI systems affecting operational safety or continuity to the BAIS;
- b. Conduct simulation-based stress testing and risk assessments;
- c. Maintain human override capabilities at all operational levels;
- d. Implement multi-layered fail-safe mechanisms and contingency plans;
- e. Submit incident reports following system disruptions or failures;
- f. Ensure resilience against cyber threats, system failures, and cascading risks.

SEC. 26. Artificial Intelligence in Media, Entertainment, and Content Generation. Entities using AI systems to generate or distribute content shall:

- a. Clearly disclose AI-generated or AI-altered content through visible and accessible labeling;
- b. Identify political, journalistic, or commercial content involving synthetic media;
- c. Prohibit impersonation of real individuals without consent;
- d. Implement safeguards against disinformation, manipulation, and harmful synthetic media;
- e. Maintain internal controls and verification mechanisms to prevent misuse.

The BAIS shall issue guidelines on labeling standards, watermarking, and content authenticity.

SEC. 27. Artificial Intelligence in Creative Industries. Entities operating in creative sectors, including film, music, literature, visual arts, gaming, and design, shall:

- a. Ensure that AI systems do not unlawfully reproduce or derive from protected intellectual property;
- b. Disclose material AI contribution in creative outputs;
- c. Maintain transparency in AI-assisted creation;
- d. Establish safeguards against unauthorized replication or deceptive representation;
- e. Respect intellectual property rights and applicable laws.

The BAIS may establish certification schemes and voluntary standards for ethical AI use in creative industries.

SEC. 28. Adaptive Governance. The provisions of this Act shall be subject to periodic review and refinement in response to technological developments, emerging risks, and societal needs. The BAIS, in coordination with relevant stakeholders, is authorized to:

- a. Issue supplemental rules and guidelines;
- b. Update risk classifications and regulatory approaches;
- c. Recommend legislative amendments where necessary;
- d. Ensure that governance frameworks remain responsive, flexible, and future-ready.

CHAPTER VI OFFENSES, PENALTIES, AND REMEDIES

SEC. 29. General Liability Framework. Any person, entity, or institution that violates any provision of this Act, whether by act or omission, shall be held liable under applicable civil, administrative, or criminal laws, depending on the nature, gravity, and consequences of the violation.

Liability shall attach regardless of whether the violation arises from the design, development, training, testing, deployment, operation, or use of an Artificial Intelligence system.

In determining the appropriate penalty or sanction, the following factors shall be considered:

- a. The level of autonomy, complexity, and risk associated with the AI system;
- b. Whether the violation was committed willfully, recklessly, negligently, or in good faith;
- c. The extent, duration, and severity of harm or rights infringement caused;
- d. The number of individuals or entities affected;
- e. The degree of control exercised by the liable party over the AI system;
- f. The existence or absence of prior compliance measures, safeguards, or due diligence;
- g. Whether the violation was self-reported or voluntarily disclosed;
- h. The timeliness and adequacy of corrective or remedial actions taken; and
- i. Any aggravating or mitigating circumstances as may be determined by the BAIS.

SEC. 30. Unauthorized Deployment of High-Risk AI Systems. The deployment, operation, or use of any high-risk Artificial Intelligence system without prior registration, classification, pre-deployment review, certification, or required documentation shall constitute a violation of this Act. Such violation shall be subject to:

- a. An administrative fine not exceeding Five Million Pesos (P5,000,000.00) per violation;
- b. Immediate suspension, restriction, or prohibition of the use of the AI system by order of the BAIS;
- c. Mandatory submission of corrective documentation, compliance reports, and risk mitigation measures within thirty (30) days; and
- d. Additional sanctions as may be imposed under applicable laws.

The BAIS may allow first-time violators to remedy noncompliance within a reasonable grace period, provided that no substantial harm has occurred, and the entity demonstrates good faith and willingness to comply.

SEC. 31. Failure to Disclose AI Use. Failure to disclose the use of Artificial Intelligence systems in contexts where disclosure is required under this Act or the CAIR shall constitute a violation. Such violation shall be subject to:

- a. An administrative fine not exceeding Two Million Pesos (P2,000,000.00);
- b. Mandatory issuance of disclosure notices to affected individuals within fifteen (15) days;
- c. Public posting of corrective statements, errata notices, or audit findings where appropriate; and
- d. Compliance monitoring by the BAIS.

Repeated violations shall be subject to increased penalties and possible suspension of AI system operations.

SEC. 32. Deployment of Prohibited AI Practices. The development, deployment, or use of Artificial Intelligence systems for prohibited purposes under this Act shall constitute a criminal offense. Such prohibited acts include, but are not limited to:

- a. Unauthorized biometric surveillance or mass profiling of individuals;
- b. Creation or dissemination of deepfake content for impersonation, fraud, or deception without consent;
- c. Use of AI systems for deceptive political influence, manipulation, or disinformation;
- d. Deployment of AI systems that exploit vulnerable populations through coercion, manipulation, or abuse; and
- e. Any AI application expressly prohibited under Section 18 of this Act.

Any person found guilty of such offenses shall suffer:

- a) Imprisonment of not less than six (6) months nor more than six (6) years; or
- b) A fine not exceeding Two Million Pesos (P2,000,000.00); or
- c) Both such imprisonment and fine, at the discretion of the court.

This shall be without prejudice to prosecution under other applicable laws, including the Revised Penal Code, Cybercrime Prevention Act, and other special laws.

SEC. 33. Corporate and Institutional Liability. Where a violation of this Act is committed by a juridical entity, including corporations, partnerships, associations, educational institutions, or public agencies, liability shall extend jointly and severally to:

- a) The entity itself;
- b) Any officer, director, or employee who authorized, directed, participated in, or knowingly allowed the violation; and
- c) The compliance officer or responsible official who failed to prevent, report, or mitigate the violation, where gross negligence or willful disregard is established.

The imposition of liability shall not preclude additional administrative, civil, or criminal actions against responsible individuals.

SEC. 34. Civil Remedies. Any person whose rights have been violated or adversely affected as a result of the unlawful deployment or use of an Artificial Intelligence system shall have the right to seek civil remedies. Such remedies may include:

- a. Injunctive relief to prevent or stop harmful AI activities;
- b. Actual damages for quantifiable losses suffered;
- c. Moral damages for emotional distress, reputational harm, or violation of dignity;
- d. Exemplary damages where the violation is attended by bad faith, malice, or gross negligence;
- e. Correction, rectification, or deletion of personal data or AI-generated outputs; and
- f. Public retraction or disclosure, where necessary to mitigate harm.

Courts shall ensure that remedies are accessible, timely, and proportionate to the harm suffered.

SEC. 35. Administrative Sanctions. In addition to fines and other penalties, the BAIS may impose administrative sanctions, including:

- a. Blacklisting of entities from government procurement, contracts, or partnerships;
- b. Public disclosure of non-compliant entities and violations;
- c. Suspension or revocation of permits, licenses, or certifications;
- d. Mandatory third-party audits, compliance reviews, or technical assessments;
- e. Imposition of operational restrictions or limitations; and
- f. Any other administrative measure necessary to ensure compliance and prevent further violations.

Administrative sanctions shall be imposed following due process and in accordance with applicable administrative procedures.

SEC. 36. Safe Harbor Protections. Individuals who, in good faith, report violations of this Act, provide information, or cooperate with investigations shall be protected from retaliation, harassment, or adverse consequences. Entities that voluntarily disclose violations, self-report noncompliance, or take prompt corrective action may, at the discretion of the BAIS:

- a. Be granted mitigation of penalties;
- b. Receive reduced fines or sanctions; or
- c. Be considered for exemption from certain enforcement actions, where appropriate.

The BAIS shall establish guidelines for whistleblower protection, voluntary disclosure, and compliance incentives.

CHAPTER VII INNOVATION, PUBLIC INFRASTRUCTURE, AND NATIONAL CAPACITY

SEC. 37. National Artificial Intelligence Infrastructure. The Department of Information and Communications Technology (DICT), through the Bureau of Artificial Intelligence Systems (BAIS), shall establish, develop, and maintain shared national infrastructure to support the ethical, secure, and inclusive development of Artificial Intelligence technologies in the Philippines. Such infrastructure shall include:

- a. *Public Computing Facilities* – High-performance computing resources, including cloud-based and on-premise systems, accessible to accredited academic institutions, research organizations, startups, and government agencies;
- b. *National Data Commons* – Curated datasets made available for AI development, subject to anonymization, privacy safeguards, ethical use, and lawful processing standards;
- c. *Open-Source AI Libraries* – Version-controlled repositories of models, tools, algorithms, and codebases for public use, testing, and innovation;
- d. *Secure Research Environments* – Controlled platforms that enable privacy-preserving data sharing, experimentation, and collaborative AI development;
- e. *Interoperable Data Systems* – Standards and platforms that facilitate secure data exchange across government agencies and authorized entities;
- f. *Cybersecurity and Resilience Systems* – Infrastructure designed to protect AI systems from cyber threats, adversarial attacks, and system failures.

The State shall prioritize equitable access to such infrastructure across regions and sectors, including underserved and geographically isolated communities.

SEC. 38. Regulatory Sandbox Programs. The BAIS shall establish and administer Regulatory Sandbox Programs to support innovation while ensuring safety and accountability. Such sandbox programs shall:

- a. Allow time-bound and supervised deployment of AI systems for research, testing, or pilot implementation;
- b. Grant conditional exemptions from specific regulatory requirements where appropriate;
- c. Require submission of detailed risk assessments, mitigation plans, and monitoring protocols;
- d. Ensure user transparency and informed participation where applicable;
- e. Be subject to clearly defined geographic, functional, or sectoral limitations;
- f. Require periodic reporting of system performance, risks, and outcomes; and
- g. Be terminated, modified, or extended based on evaluation results and compliance.

The BAIS shall publish guidelines governing sandbox participation, evaluation criteria, and exit conditions.

SEC. 39. Support for Domestic Artificial Intelligence Development. The State shall promote the development of locally designed and developed Artificial Intelligence systems, particularly those aligned with national priorities, cultural contexts, and linguistic diversity.

Support mechanisms shall include:

- a. Grants, subsidies, and challenge programs to encourage innovation in AI;
- b. Preferential funding and procurement for locally developed AI solutions;
- c. Technical assistance and incubation programs for startups and MSMEs;
- d. Incentives for private sector investment in AI research and development;
- e. Support for the development of AI models in Philippine languages and dialects;
- f. Promotion of inclusive participation in AI innovation ecosystems, including women, youth, and marginalized sectors.

Government agencies shall coordinate to ensure that domestic AI development is aligned with ethical standards, safety requirements, and national development goals.

SEC. 40. National Artificial Intelligence Research and Testing Facilities. The DICT, in coordination with the Department of Science and Technology (DOST), shall establish National Artificial Intelligence Research and Testing Centers to serve as independent and neutral platforms for:

- a. Model validation, evaluation, and certification;
- b. Bias detection, fairness assessment, and safety testing;
- c. Benchmarking of AI system performance against national and international standards;
- d. Training and capacity-building for regulators, public officials, and technical personnel;
- e. Research on emerging AI technologies, risks, and societal impacts.

These facilities shall be accessible to public agencies, academic institutions, and qualified private entities, subject to regulatory guidelines.

SEC. 41. AI Education, Talent Development, and Workforce Transition. The Commission on Higher Education (CHED), in coordination with the BAIS, shall develop and implement curriculum standards, academic programs, and faculty development initiatives to promote Artificial Intelligence literacy, ethics, and technical competencies. Such initiatives shall include:

- (a) Undergraduate and graduate degree programs in Artificial Intelligence, data science, and related disciplines;
- (b) Integration of ethical AI principles across technical and non-technical fields of study;
- (c) Scholarships, grants, and fellowships for students and researchers in AI-related fields;

- (d) Training-of-trainers programs to enhance faculty capacity;
- (e) Partnerships with industry, international institutions, and research organizations.

The State shall likewise implement workforce transition programs to address the impact of AI on employment, including reskilling and upskilling programs for affected workers; job transition support and placement services; monitoring of labor market trends and emerging skill demands; and promotion of inclusive participation in AI-related industries. The Department of Labor and Employment (DOLE), in coordination with CHED, TESDA, and the BAIS, shall lead workforce transition initiatives.

SEC. 42. Technology Transfer and Knowledge-Sharing. The DICT shall establish policies and mechanisms to promote technology transfer and knowledge-sharing from foreign entities operating Artificial Intelligence systems in the Philippines. Such mechanisms may include:

- i. Disclosure of relevant model characteristics, documentation, and performance metrics;
- ii. Publication of localized testing results and evaluations;
- iii. Sharing of best practices, tools, and safety frameworks;
- iv. Capacity-building partnerships with local institutions;
- v. Conditions for participation in public procurement or sandbox programs.

Foreign entities that fail to meet minimum transparency and accountability requirements may be restricted from participating in government-funded AI programs or deployments.

SEC. 43. Artificial Intelligence Safety Research Fund. There is hereby created an Artificial Intelligence Safety Research Fund, to be administered by the BAIS and funded through annual appropriations. The Fund shall support:

- (a) Independent safety evaluations and risk assessments of AI systems;
- (b) Research on bias detection, mitigation, and fairness;
- (c) Red-teaming, adversarial testing, and security analysis;
- (d) Academic, technical, and policy research on long-term AI risks and governance;
- (e) Development of national safety benchmarks and standards.

The BAIS shall establish transparent guidelines for the allocation, use, and monitoring of the Fund.

CHAPTER VIII

ROLES OF NATIONAL GOVERNMENT AGENCIES

SEC. 44. Role of the Department of Information and Communications Technology. The Department of Information and Communications Technology (DICT) shall serve as the principal agency responsible for the implementation of this Act.

Through the Bureau of Artificial Intelligence Systems (BAIS), the DICT shall exercise regulatory, administrative, investigatory, and enforcement functions over Artificial Intelligence systems in the Philippines.

The DICT shall ensure policy coherence, inter-agency coordination, and alignment of AI governance with national digital transformation strategies.

SEC. 45. Role of the Department of Science and Technology. The Department of Science and Technology (DOST) shall support the implementation of this Act by:

- (a) Providing funding, technical expertise, and research infrastructure for AI development;
- (b) Supporting the establishment of National AI Research and Testing Centers;
- (c) Promoting scientific research in AI applications across sectors such as healthcare, agriculture, climate, and disaster risk reduction;

- (d) Developing science-based evaluation frameworks for AI performance, safety, and bias detection.

SEC. 46. Role of the Commission on Higher Education. The Commission on Higher Education (CHED) shall:

- a. Integrate Artificial Intelligence into higher education curricula;
- b. Establish academic standards for AI-related degree programs;
- c. Recognize centers of excellence in AI education and research;
- d. Promote postgraduate research aligned with national AI priorities.

SEC. 47. Role of the Department of Trade and Industry. The Department of Trade and Industry (DTI) shall:

- a. Promote responsible adoption of AI in the private sector;
- b. Support MSMEs in adopting AI technologies;
- c. Encourage the development of export-ready and globally competitive AI products;
- d. Coordinate with the BAIS in establishing sector-specific standards and compliance support mechanisms.

SEC. 48. Role of the Department of Health. The Department of Health (DOH) shall:

- a. Ensure that AI systems used in healthcare are safe, ethical, and compliant with medical standards;
- b. Approve and regulate AI systems used for diagnosis, treatment, and clinical decision-making in coordination with the BAIS;
- c. Monitor post-deployment effects of AI on public health;
- d. Participate in regulatory sandbox programs for healthcare AI.

SEC. 49. Role of the Department of Education. The Department of Education (DepEd) shall:

- a. Ensure ethical integration of AI in basic education;
- b. Protect students from harmful or biased AI applications;
- c. Establish standards for AI use in instruction, grading, and administration;
- d. Promote AI literacy and digital competency among learners.

SEC. 50. Role of the Department of Labor and Employment. The Department of Labor and Employment (DOLE) shall:

- (a) Monitor the impact of AI on employment, wages, and working conditions;
- (b) Develop policies to ensure fairness in AI-assisted recruitment and evaluation;
- (c) Lead workforce transition, reskilling, and upskilling programs;
- (d) Protect workers from discriminatory or exploitative AI practices.

SEC. 51. Role of the National Privacy Commission. The National Privacy Commission (NPC) shall:

- (a) Ensure that AI systems comply with the Data Privacy Act of 2012;
- (b) Provide guidance on consent, lawful processing, and data minimization;
- (c) Issue joint guidelines with the BAIS on AI-related privacy issues;
- (d) Monitor risks arising from automated processing and profiling.

SEC. 52. Role of the Philippine Statistics Authority. The Philippine Statistics Authority (PSA) shall:

- (a) Ensure that datasets used for AI development are accurate, representative, and ethically released;
- (b) Support the creation of the National Data Commons;
- (c) Assist in structuring and documenting datasets for lawful reuse;
- (d) Report risks and impacts arising from AI use of PSA-managed data.

SEC. 53. Role of the Department of Economy, Planning, and Development.

The Department of Economy, Planning, and Development (DEPDev) shall:

- a. Integrate AI into national development planning;
- b. Assess the economic and social impact of AI adoption;
- c. Support investment strategies aligned with AI innovation;
- d. Include AI policy considerations in the Philippine Development Plan.

SEC. 54. Role of the Department of Justice.

The Department of Justice (DOJ) shall:

- a. Provide legal guidance on rights and remedies related to AI;
- b. Develop prosecutorial frameworks for AI-related offenses;
- c. Ensure that constitutional guarantees such as due process and equal protection are upheld in AI governance.

SEC. 55. Role of the Judiciary. The Judiciary shall be encouraged to:

- a. Develop policies on the admissibility and use of AI-generated evidence;
- b. Ensure fairness and due process in AI-assisted judicial proceedings;
- c. Build institutional capacity to understand and evaluate AI technologies.

SEC. 56. Role of the Department of Foreign Affairs. The Department of Foreign Affairs (DFA) shall:

- a. Represent the Philippines in international AI governance discussions;
- b. Promote national interests in global standards, treaties, and cooperation;
- c. Coordinate with the BAIS on international partnerships.

SEC. 57. Role of the Department of the Interior and Local Government. The Department of the Interior and Local Government (DILG) shall:

- (a) Supervise AI deployment by local government units;
- (b) Ensure compliance of local AI initiatives with this Act;
- (c) Provide guidance and oversight to LGUs.

SEC. 58. Role of the National Telecommunications Commission. The National Telecommunications Commission (NTC) shall:

- (a) Oversee AI use by telecommunications providers;
- (b) Ensure that AI-enabled practices do not result in discrimination, manipulation, or unfair access;
- (c) Coordinate with the BAIS on reporting and compliance requirements.

SEC. 59. Role of the Civil Service Commission. The Civil Service Commission (CSC) shall:

- (a) Ensure ethical use of AI in public sector human resource management;
- (b) Promote merit, transparency, and fairness in AI-assisted personnel decisions;
- (c) Support capacity-building for civil servants in AI governance.

SEC. 60. Role of the Commission on Elections. The Commission on Elections (COMELEC) shall:

- (a) Regulate AI use in electoral processes and campaign activities;
- (b) Prevent AI-driven voter manipulation, disinformation, and impersonation;

(c) Coordinate with the BAIS on approval of AI use in elections.

SEC. 61. Role of the Anti-Red Tape Authority. The Anti-Red Tape Authority (ARTA) shall:

- (a) Promote AI use to streamline public services;
- (b) Ensure that AI systems improve efficiency without causing exclusion or discrimination;
- (c) Align AI adoption with ease-of-doing-business objectives.

SEC. 62. Role of the Department of Budget and Management. The Department of Budget and Management (DBM) shall:

- (a) Ensure that AI-related funding requests include risk assessments and compliance documentation;
- (b) Support budget allocation for AI programs and infrastructure;
- (c) Coordinate with the BAIS to prioritize investments aligned with national AI goals.

CHAPTER IX EMERGING TECHNOLOGIES, PUBLIC SAFETY, AND ADAPTIVE MEASURES

SEC. 63. Transitory Exercise of Powers. Until the Bureau of Artificial Intelligence Systems (BAIS) is fully constituted, the Secretary of the Department of Information and Communications Technology (DICT) shall exercise the powers, duties, and functions of the Bureau under this Act in an ex officio capacity. In the exercise of such powers, the Secretary shall apply the precautionary principle, risk-based regulation, and ethical safeguards established under this Act.

The Secretary may designate an interim office, unit, or officer within the DICT to carry out the operational functions of the BAIS during the transition period.

SEC. 64. Authority to Address Emerging Risks. The BAIS is hereby authorized to issue precautionary advisories, interim regulatory measures, or temporary restrictions in response to emerging Artificial Intelligence applications that present new, unregulated, or escalating risks to:

- (a) Human rights and civil liberties;
- (b) Public health and safety;
- (c) National security;
- (d) Democratic institutions and processes; or
- (e) Economic stability and market integrity.

Such measures may include:

- (1) Temporary suspension of deployment;
- (2) Imposition of additional safeguards or compliance requirements;
- (3) Mandatory reporting or monitoring obligations; or
- (4) Time-bound moratoriums.

Emergency measures issued under this Section shall not exceed twelve (12) months in duration unless extended or replaced by formal regulation.

SEC. 65. Artificial Intelligence Applications in Policing and Public Order. No Artificial Intelligence system shall be deployed for policing, crime prediction, crowd monitoring, automated enforcement of laws, or similar public order functions without prior approval from the BAIS.

Such approval shall be granted only upon compliance with the following:

- a. Coordination with the Department of the Interior and Local Government (DILG) and, where appropriate, the Commission on Human Rights (CHR);

- b. Clear demonstration of necessity, proportionality, and lawful purpose;
- c. Implementation of strict safeguards to protect civil liberties, due process, and privacy rights;
- d. Assurance of continuous human oversight and decision-making authority;
- e. Transparency measures, including public disclosure where feasible and lawful;
- f. Independent post-deployment evaluation and audit.

The use of AI systems for real-time facial recognition, predictive policing, behavioral profiling, or mass surveillance shall be presumed high-risk and shall not be permitted unless specifically authorized by law; subject to judicial oversight; and compliant with strict safeguards and limitations.

The BAIS may suspend or revoke approval for any system found to undermine constitutional rights or public trust.

SEC. 66. Experimental Artificial Intelligence Systems. The BAIS may authorize the deployment of experimental or novel AI systems through regulatory sandbox programs. Such authorization shall be subject to:

- a. Submission of detailed risk documentation and system specifications;
- b. Implementation of safeguards for user protection, including transparency and informed participation;
- c. Continuous monitoring and reporting requirements;
- d. Defined geographic, sectoral, or operational limits;
- e. Time-bound deployment with clear evaluation criteria.

The BAIS may terminate or suspend experimental deployments at any time where risks exceed acceptable thresholds.

SEC. 67. Artificial Intelligence Systems Exhibiting Unanticipated or Emergent Behavior. Any person or entity responsible for deploying an AI system that exhibits unanticipated, self-modifying, emergent, or unpredictable behavior shall:

- (a) Immediately report such behavior to the BAIS;
- (b) Implement containment, suspension, or mitigation measures;
- (c) Provide full technical documentation and system logs for review;
- (d) Cooperate with investigations and safety assessments.

The BAIS may require the suspension, modification, or withdrawal of such systems pending evaluation. AI systems demonstrating emergent behavior shall not be permitted to operate autonomously in high-risk domains, including:

- (1) Healthcare;
- (2) Law enforcement;
- (3) National defense;
- (4) Critical infrastructure.

SEC. 68. Systemic Failure and Emergency Response Planning. The BAIS, in coordination with the National Disaster Risk Reduction and Management Council (NDRRMC) and other relevant agencies, shall establish a national contingency framework for systemic AI failures.

Such framework shall include:

- (a) Procedures for responding to large-scale AI system failures or disruptions;
- (b) Mechanisms for detecting and containing cascading failures across interconnected systems;
- (c) Protocols for addressing adversarial attacks, misinformation campaigns, and coordinated AI misuse;
- (d) Emergency shutdown or “kill-switch” mechanisms for high-impact AI systems;
- (e) Coordination strategies among public and private stakeholders during crisis situations.

Entities operating high-risk AI systems shall be required to maintain internal emergency response plans aligned with this framework.

SEC. 69. Artificial Intelligence in Financial Systems and Systemic Market Risks. AI systems used in banking, insurance, securities trading, asset management, or financial infrastructure shall be subject to enhanced oversight.

The BAIS, in coordination with the Bangko Sentral ng Pilipinas (BSP), the Securities and Exchange Commission (SEC), and the Insurance Commission, shall:

- a. Require pre-deployment review and stress testing of high-risk financial AI systems;
- b. Ensure that such systems do not create excessive volatility, herding behavior, or systemic contagion;
- c. Mandate algorithmic transparency sufficient for regulatory oversight;
- d. Require reporting of anomalies or failures affecting financial stability;
- e. Ensure the presence of circuit breakers, fail-safe mechanisms, and human override capabilities.

Financial institutions shall be held accountable for AI-driven outcomes that materially affect markets, consumers, or financial systems.

SEC. 70. Future Preparedness and Foresight Mechanisms. The BAIS shall establish a permanent foresight and strategic assessment unit to monitor global trends in advanced Artificial Intelligence.

Such unit shall:

- a. Conduct scenario planning on emerging technologies, including Artificial General Intelligence (AGI), autonomous systems, and advanced generative models;
- b. Assess long-term risks to society, governance, labor, and national security;
- c. Monitor international regulatory developments and best practices;
- d. Publish periodic foresight reports and recommendations;
- e. Submit a comprehensive strategic risk report to Congress every four (4) years.

The State shall ensure that governance frameworks remain adaptive, forward-looking, and capable of addressing future technological developments.

CHAPTER X NATIONAL PANEL OF EXPERTS ON ARTIFICIAL INTELLIGENCE

SEC. 71. Creation of the National Panel of Experts and Resource Persons on Artificial Intelligence (NPER-AI). There is hereby established an independent, multisectoral, and consultative body to be known as the National Panel of Experts and Resource Persons on Artificial Intelligence (NPER-AI).

The Panel shall serve as an institutional advisory mechanism to the Bureau of Artificial Intelligence Systems (BAIS), providing independent ethical, technical, and public interest perspectives on matters relating to Artificial Intelligence governance in the Philippines.

The Panel shall function in an advisory capacity and shall not exercise regulatory or enforcement powers, but its recommendations shall carry persuasive authority and shall be given due consideration by the BAIS and other government agencies.

SEC. 72. Mandate and Functions. The NPER-AI shall perform the following functions:

- (a) Provide ethical oversight and issue non-binding advisory opinions on Artificial Intelligence systems, regulatory actions, or policies that raise novel, high-risk, or controversial concerns;
- (b) Review and provide recommendations on proposed regulations, standards, and major AI deployments referred by the BAIS;
- (c) Facilitate public engagement through consultations, hearings, forums, and dialogues on Artificial Intelligence governance;
- (d) Conduct independent studies and foresight assessments on emerging risks, societal impacts, and ethical implications of AI;
- (e) Prepare and submit an Annual AI Ethics and Public Impact Report to the President, Congress, the BAIS, and the public;
- (f) Promote awareness and understanding of ethical AI principles among stakeholders;
- (g) Serve as a platform for interdisciplinary collaboration among experts, civil society, academia, and industry.

Where the BAIS adopts a position contrary to a formal recommendation of the Panel, the Bureau shall provide a written explanation of its rationale.

SEC. 73. Composition and Appointment. The National Panel of Experts and Resource Persons on Artificial Intelligence shall be composed of nine (9) members, appointed by the President of the Philippines upon recommendation of the Secretary of Information and Communications Technology.

The Panel shall be composed of individuals representing diverse fields of expertise and public interest perspectives, including:

- a. One (1) Artificial Intelligence researcher or machine learning expert;
- b. One (1) ethicist, philosopher, or religious scholar with demonstrated expertise in technology ethics;
- c. One (1) representative from the labor sector, preferably from a recognized national labor organization;
- d. One (1) legal expert specializing in human rights, data privacy, or technology law;
- e. One (1) sociologist, anthropologist, or public interest technologist;
- f. One (1) representative from the youth or academic sector, preferably under the age of thirty (30);
- g. One (1) regional representative from the Visayas or Mindanao, on a rotating basis every three (3) years;
- h. One (1) representative from the private sector, preferably from a startup, MSME, or innovation-driven enterprise;
- i. One (1) media practitioner, journalist, or researcher with expertise in disinformation, digital media, or information integrity.

Members shall be selected based on competence, integrity, independence, and commitment to the public interest.

SEC. 74. Term of Office, Compensation, and Qualifications. Members of the Panel shall serve a term of three (3) years, renewable for one (1) additional term.

Members shall receive honoraria, allowances, and such other compensation as may be determined by the Department of Budget and Management, subject to existing laws, rules, and availability of funds.

No person shall be appointed as a member of the Panel if they:

- (a) Hold a position that creates a conflict of interest with the functions of the Panel;
- (b) Have been convicted of a crime involving moral turpitude;
- (c) Are directly engaged in activities that may compromise their independence.

Members shall disclose any potential conflicts of interest and shall recuse themselves from deliberations where such conflicts exist.

SEC. 75. Secretariat and Administrative Support. The National Panel of Experts and Resource Persons on Artificial Intelligence shall be supported by a Secretariat to be provided by the Department of Information and Communications Technology, in coordination with the BAIS.

The Secretariat shall:

- (a) Provide technical, research, and administrative assistance to the Panel;
- (b) Organize meetings, consultations, and public engagement activities;
- (c) Facilitate the preparation and publication of reports, recommendations, and advisory opinions;
- (d) Maintain records and documentation of Panel activities.

The Secretariat shall operate in a manner that preserves the independence, integrity, and effectiveness of the Panel.

CHAPTER XI TRANSITION, IMPLEMENTATION, AND FINAL PROVISIONS

SEC. 76. Appropriations. The amount necessary for the initial implementation of this Act shall be charged against the current appropriations of the Department of Information and Communications Technology (DICT).

Thereafter, such sums as may be necessary for the continued implementation of this Act, including the operation of the Bureau of Artificial Intelligence Systems (BAIS), the National AI Infrastructure, research programs, and other initiatives provided herein, shall be included in the annual General Appropriations Act.

SEC. 77. Organizational Transition. Within ninety (90) days from the effectivity of this Act, the DICT shall:

- a. Establish the organizational structure, staffing pattern, and operational framework of the BAIS;
- b. Reorganize existing units or offices within the DICT engaged in Artificial Intelligence, data governance, or digital regulation into the BAIS;
- c. Appoint or designate interim officers and personnel necessary for the initial operations of the Bureau;
- d. Ensure compliance with civil service laws, rules, and regulations in the establishment of positions.

Pending the full establishment of the BAIS, the Secretary of the DICT shall exercise all powers and functions of the Bureau and may designate an interim office or officer to perform its duties.

SEC. 78. Publication of the Code of Artificial Intelligence Regulations (CAIR). Within one hundred eighty (180) days from the effectivity of this Act, the BAIS shall promulgate and publish the initial version of the Code of Artificial Intelligence Regulations (CAIR) which shall contain:

- a. Technical standards and compliance requirements;
- b. Risk classification frameworks;
- c. Registration procedures for AI systems;
- d. Documentation and audit requirements;
- e. Sector-specific guidelines;
- f. Enforcement mechanisms and administrative procedures.

The CAIR shall be periodically reviewed and updated to reflect technological developments and regulatory needs.

SEC. 79. Annual Reporting and Congressional Review. The BAIS shall submit an annual report to Congress, which shall include:

- (a) Status of AI system registrations and deployments;
- (b) Results of compliance monitoring and enforcement actions;
- (c) Emerging risks, trends, and technological developments;
- (d) Impact of AI on economic, social, and governance sectors;
- (e) Recommendations for legislative or regulatory improvements.

Congress shall conduct a comprehensive review of this Act every three (3) years and may amend, revise, or expand its provisions as necessary.

SEC. 80. Implementing Rules and Regulations. Within ninety (90) days from the effectivity of this Act, the DICT, in coordination with the BAIS and relevant government agencies, shall promulgate the necessary Implementing Rules and Regulations (IRR).

In formulating the IRR, the DICT shall consult the National Privacy Commission (NPC); the Department of Justice (DOJ); the Civil Service Commission (CSC); and other relevant agencies, stakeholders, and experts.

The IRR shall take effect fifteen (15) days after publication in the Official Gazette or in a newspaper of general circulation.

SEC. 81. Repealing Clause. All laws, decrees, executive orders, rules and regulations, or parts thereof inconsistent with the provisions of this Act are hereby repealed, amended, or modified accordingly.

SEC. 82. Suppletory Clause. This Act shall be construed in harmony with existing laws on data privacy, cybersecurity, public accountability, procurement, and sectoral regulation.

In particular, Republic Act No. 10173, or the Data Privacy Act of 2012, shall apply in a suppletory manner.

Nothing in this Act shall be construed to prohibit algorithmic audits, bias testing, red-teaming, or evaluation processes required under this Act, provided that such activities are conducted in accordance with lawful processing, proportionality, and appropriate safeguards.

SEC. 83. Separability Clause. If any provision, section, or part of this Act is declared unconstitutional or invalid, such declaration shall not affect the validity of the remaining provisions, which shall continue to be in full force and effect.

SEC. 84. Effectivity Clause. This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in a newspaper of general circulation.

Approved,