Introduction

Artificial intelligence (AI) technology is a central, active, and critically important element in the evolution of our world today, which has become increasingly and rapidly digital. This technology is reshaping our societies worldwide and redefining our perceptions of future economic and social development.

At the same time, it presents humanity with some of the most challenging dilemmas in our history. As great as the promises this technology offers, the threats it poses are equally significant, with some believing it may even pose an existential threat to humanity itself.

Regardless of how exaggerated some positive or negative perceptions may be, this technology's importance for any society's future cannot be underestimated. Therefore, regulating the development and use of AI is an urgent necessity for any society today. Regulation is the only tool that can ensure the maximum developmental benefits of this technology while protecting the rights of individuals and institutions against the threats arising from its negative impacts.

State institutions in Egypt have shown interest in AI's potential to achieve developmental goals. This has been reflected in establishing the National Council for Artificial Intelligence and issuing several important documents, including the National Artificial Intelligence Strategy and the Egyptian Charter for Responsible AI. According to the latest edition of the National AI Strategy, a draft law is currently being prepared to regulate AI in Egypt.

Given the strategic importance of regulating the use of AI, "*Masaar*" is taking the initiative through this policy paper to propose criteria for evaluating this legislation. These criteria are built on *Masaar*'s previous efforts in studying the various aspects of AI, particularly its potential impacts on fundamental rights. They are also based on the papers *Masaar* has published addressing the requirements for regulatory frameworks for AI and its proposal of the fundamental principles for the ethical governance of AI.

This paper is structured in three primary sections. Section one examines the broader legislative frameworks governing AI usage in Egypt, exploring the legislative, regulatory, and knowledge contexts in which this law will operate. This section also analyzes the law's underlying philosophy, vision, goals, and the most effective approaches for achieving its intended outcomes.

Section two focuses on establishing general evaluation criteria for the legislation and identifying the core principles that inform the detailed assessment metrics. The final section presents specific evaluation criteria for the law's provisions, encompassing both general stipulations and the particular obligations that should be placed on AI system service providers.

The Legislative Environment

The Relevant Local Laws in Force:

Personal Data Protection Law No. 151 of 2020

AI systems are the most data-dependent among all types of software. Modern AI models rely heavily on the intensive use of data during the stages of their development, preparation for deployment, and actual use. Violations and risks related to the collection, storage, processing, and exchange of data represent the primary source of concerns and warnings regarding the development and use of AI systems.

Therefore, a personal data protection law is an essential pillar of the legislative environment necessary for regulating AI technology. Consequently, any specialized legislative framework regulating this technology should closely integrate with the Personal Data Protection Law and avoid any conflicts with it.

Additionally, this legislation should avoid leaving loopholes where the two laws might overlap, leading to legislative duplication, or where neither applies, allowing certain practices to escape regulatory oversight.

Regulatory Framework for Data Centers (2021)

The National Telecom Regulatory Authority (NTRA) adopted this regulatory framework in August 2021. Data centers are high-tech facilities housing equipment and devices for storing and processing big data. They provide massive storage capacities and significant processing capabilities, especially if some of their servers are equipped with specialized electronic chips.

These centers are essential for operating AI systems locally, particularly in all non-personal or limited experimental use cases. Therefore, the law should ensure that entities developing,

deploying, and operating AI systems locally comply with this regulatory framework. Additionally, it is crucial to prevent any conflicts between the provisions of the law and this framework.

The Anti-Cyber and Information Technology Crimes Law No. 175 of 2018

The AI law must align with this legislation by ensuring that AI system practices do not constitute criminal acts or serve as tools for committing cybercrimes as defined by the law. Furthermore, the law should mandate that those operating and deploying AI systems via information systems adhere to the information security and unauthorized access regulations outlined in the Anti-Cybercrime Law.

Other Relevant Laws Regulating the Use of AI Systems

In addition to the aforementioned laws, the following laws regulate areas related to the various uses of AI systems. They also constitute essential elements in the legislative environment with which the AI regulation law should align and integrate.

- Consumer Protection Law No. 181 of 2018.
- Telecommunications Regulation Law No. 10 of 2003.
- Law Regulating the Use of Financial Technology in Non-Banking Financial Activities No. 5 of 2022.
- Electronic Signature Regulation Law No. 15 of 2004.
- Intellectual Property Rights Protection Law No. 82 of 2002.

Shortcomings and Deficiencies

Several deficiencies in the Egyptian legislative environment could hinder the achievement of the goals of the AI regulation law. Some of the most important of these deficiencies are as follows:

Failure to Issue the Executive Regulations for the Personal Data Protection Law

Despite nearly five years having passed, the Egyptian government has not yet issued the executive regulations for the Personal Data Protection Law. Given that this law delegates the regulation of a significant portion of its rules and procedures to its executive regulations, the possibility of enforcing its provisions in their absence is virtually nonexistent.

This means that, at present, the law is effectively inoperative in practice. This leaves many loopholes that the AI law cannot cover, even though they are essential for its operation and achieving its objectives.

Absence of Legislation to Regulate Digital Services

The term "digital services" encompasses a wide range of services provided to users over the Internet. Prominent examples include social media platforms, search engines, instant messaging services, remote working websites, and more.

These services increasingly and intensively use AI systems. In recent years, services that provide direct access to AI models via chatbot applications based on language models have also emerged.

These services allow using AI models to analyze information, prepare reports and academic papers, write software codes, and do countless other tasks. Regulating the operation of such services intersects with the goals of AI regulation. Therefore, the absence of such regulation leaves numerous loopholes that a specialized AI law cannot cover.

Absence of Legislation to Regulate E-Commerce and Digital Marketing

The regulation of e-commerce and online shopping is closely linked to the regulation of digital services and consumer protection laws. However, e-commerce activities have unique characteristics that necessitate detailed and independent regulation.

E-commerce and digital marketing activities rely heavily on AI systems. Thus, regulating this field is essential to complete the legislative environment where a specialized AI law can achieve its objectives.

Regulatory Environment

Existing Institutions and Authorities

- **Ministry of Communications and Information Technology:** This is the main government body responsible for guiding Egypt's digitalization process and technological

development. The ministry is responsible for developing national strategies to adopt AI technologies across various sectors of work in Egypt. It is also tasked with supporting government and private projects and initiatives that leverage AI to drive economic development.

- **National Council for Artificial Intelligence:** This is a body affiliated with the Cabinet. The council is chaired by the Minister of Communications and Information Technology and includes several ministers, heads of relevant authorities, as well as three experts. The council aims to review the National AI Strategy and oversee its implementation. It was also responsible for launching the second version of the National AI Strategy.
- **Information Technology Industry Development Agency (ITIDA):** The agency supports the technology and innovation sector. It also provides technical and financial support to startups in the information technology sector, including those developing AI applications.
- **The Personal Data Protection Center:** This is a public entity mandated by the Personal Data Protection Law. However, the center has not yet been established due to the delay in issuing the executive regulations. According to Article No. 19 of the law, the center is responsible for developing and implementing policies, strategic plans, and programs necessary to protect personal data. It is also tasked with unifying policies and plans for protecting and processing personal data within Egypt, as well as setting and enforcing decisions, controls, measures, procedures, and standards related to personal data protection.

Knowledge Environment

The knowledge environment refers to the sources of information and prior experiences that legislators can rely on during drafting, discussing, approving, and implementing legislation. The available body of knowledge on AI is vast and growing rapidly, making it unrealistic to fully encompass or review all the content it offers.

The practical alternative is to leverage the prior efforts of local and international entities that have introduced either regulatory frameworks for AI technology or guidelines and recommendations for its governance. The following section highlights some of the most comprehensive efforts.

International Legislative Experiences

- **The European Union AI Act:** This law is considered the first comprehensive legislative framework aimed at regulating the use of AI across all EU member states. To date, it remains the only one of its kind. The law adopts a risk-based approach, imposing requirements and obligations that vary according to the potential risks posed by AI systems. It also serves as a strong model for balancing the promotion of AI development and applications with safeguarding rights and freedoms against potential risks associated with this technology.

- **United States of America:** The U.S. legislative authorities have not yet enacted a comprehensive law to regulate the use of AI. Instead, several initiatives have emerged to address specific aspects of AI technology, including the Algorithmic Accountability Act. This proposed legislation aims to enhance algorithmic transparency, enable oversight, and hold its developers and deployers accountable.

Contributions of International Institutions

- **United Nations:** In March 2024, the General Assembly adopted a resolution to promote safe, trustworthy, and sustainable AI technologies for all. The UN's guidelines for AI governance include a set of principles such as: protecting human rights and inclusivity, transparency and explainability, accountability and distribution of responsibilities, and international cooperation to establish unified standards. Additionally, UNESCO has issued recommendations on the ethics of AI in 2021.
- **Organization for Economic Co-operation and Development (OECD):** The OECD has issued principles for the use and development of AI. Among the most important principles are: inclusive growth, sustainable development, and well-being; human-centered values and fairness; transparency and explainability; security and safety; and accountability.

Civil Society Contributions

Civil society organizations worldwide have made numerous contributions to knowledge about AI, its uses, and potential negative impacts on rights and freedoms. Many of these organizations have also proposed standards that should be included in the regulatory and legislative frameworks necessary to govern and regulate this technology.

On the local level, "Masaar" has introduced several papers and reports on AI. In particular, these papers have discussed "Regulating AI: Approaches to Ensuring the Safe Use of the Technology" and "An Approach to AI Governance: Essential Frameworks for Promoting Justice and Protecting Human Rights." Additionally, one of Masaar's papers provided a critical analysis of the European Union AI Act.

Philosophy and Approaches of the Law

Philosophy and Vision

Regulating a technology with such a broad and profound impact as AI necessitates the drafting and enacting of strategic legislation. This means that the legislation should be based on a vision encompassing all long-term ambitions for using this technology, as well as all the expected and potential consequences of its use, whether positive or negative.

This legislation should closely integrate with the state's AI strategy, serving as a key tool to achieve its objectives. The appropriate vision for this law is to encourage and drive the development of AI applications within Egypt safely and reliably while safeguarding the rights and interests of citizens and public and private institutions.

The legislation should explicitly declare its philosophy and vision through its explanatory memorandum or the text of its articles. This is essential to ensure that those subject to the law can understand the overarching framework that governs its provisions, which in turn aids in correctly interpreting them. Additionally, the philosophy and vision of the law clarify the required spirit for its enforcement authorities to apply its provisions in practice effectively.

Objectives

The objectives of the law serve as the bridge between its philosophy and vision and their translation into its texts and provisions. Explicitly stating the objectives that the law seeks to achieve is crucial for facilitating its understanding by the various parties involved in its implementation. Several considerations should be taken into account when drafting these objectives, including:

- **Clarity, Consistency, and Alignment with Philosophy and Vision:** Clarity of objectives means drafting each objective to avoid ambiguity, which could lead to multiple interpretations or contradictions. Consistency refers to the integration of objectives and avoiding any conflicts between them. Achieving both considerations depends on how well the objectives align with the law's philosophy and vision, ensuring they faithfully reflect them.
- **Comprehensiveness and Balance:** The law's objectives should cover the full scope of its application. This means the objectives should address all expected and potential uses of AI and all forms of its economic and social impacts. Additionally, the objectives should clarify the balance between encouraging the development and use of AI, maximizing its positive effects, and providing protection against its potential negative impacts.
- **Prioritization**: The objectives should reflect a clear hierarchy based on several priorities and explicit biases. In particular, the objectives should prioritize protecting citizens' fundamental rights over the economic interests of institutions in cases where the two conflict.

Approaches

This section discusses three optimal approaches that the law can adopt to achieve its objectives. It also presents criteria for evaluating the law's adherence to these approaches.

Risk-Based Approach: Graduated Requirements and Obligations

AI is inherently broad in scope and highly diverse. Therefore, it is essential for legislation regulating it to adopt an approach based on graduated requirements and obligations. This approach is seen as the most effective way to balance the need to maximize economic and social development with the need to protect the rights of individuals and institutions from the potential risks of developing and using AI.

Adopting the principle of potential risk as the basis for graduated requirements and obligations is ideal and necessary for this law. This is because clear criteria can be established to classify AI systems based on the potential risks associated with their development and use. Additionally, the different levels of risk can determine the specific requirements and obligations of entities involved in developing and deploying these systems.

Conditional Flexibility in Implementation

Conditional flexibility refers to providing regulatory and oversight bodies with a degree of freedom to act within specific and clear conditions. This approach is essential for legislation dealing with a constantly and rapidly evolving phenomenon to ensure that the law remains applicable to new developments in this field.

This approach requires that some provisions be comprehensive while allowing a certain degree of flexibility and discretion for relevant regulatory and oversight bodies to determine the applicability of the law to new emerging cases. However, this discretion must be governed by clear rules that these bodies must adhere to when exercising their roles.

The Adaptability Approach

Adaptability is essential when dealing with a technology that evolves rapidly and in unpredictable directions over the medium and long term. This technology has wide-ranging economic and social impacts, meaning that the surrounding environment must also evolve rapidly. Therefore, any flexibility in legislation regulating this technology has practical limits that prevent it from keeping pace with its long-term evolution.

Thus, the legislation itself must be open to review and development over time. To ensure that this process of evolution takes place smoothly and effectively, the legislation should regulate it and establish the appropriate conditions and procedures. This includes identifying the entities responsible for conducting regular or as-needed reviews and suggesting the necessary amendments.

General Standards and Fundamental Principles

General Standards

This section discusses a set of general standards for evaluating the text and provisions of the law. These standards apply to all legal provisions rather than a specific subset. The general standards include the following:

Language

The clarity of the language used, and the precision of wording are fundamental general standards for evaluating any legislative text. However, the specific context of regulatory law for an advanced and continuously evolving technology such as AI introduces additional considerations to meet these standards, including:

- **Technical Terminology Control:** Any specialized technical term should be accurate and consistent with its correct usage in practical contexts.
- **Providing Clear Definitions for Technical Terms:** The law should include a definitions section that clearly defines all the technical terms used within it, ensuring the accuracy and comprehensiveness of these definitions. If necessary, an index of terms in Arabic alongside their English equivalents could be added as an annex to the law. This could assist the law's addressees, particularly technical experts, and professionals accustomed to using these terms in English due to the nature of their work.
- **Consistency in technical terms:** No more than one term should refer to the same meaning in different places in the text.

Comprehensiveness

The law regulating AI should be comprehensive. This means that the law must cover all aspects relevant to its regulatory scope, including the following:

- The text of the law should encompass all potential future scenarios for using AI within its legal jurisdiction.
- The law should address all stages of designing, developing, deploying, distributing, and using AI systems.
- Ensuring that the text of the law fulfills all considerations necessary to achieve its objectives in its detailed provisions and wording. This means that the text should not overlook or contradict these considerations.

Limits of Referral to the Executive Regulations

Previous experiences have shown that unjustified expansion of delegating the completion of rules and procedures to the executive regulations carries significant drawbacks. Among these drawbacks is the practical application of the law being contingent on the political considerations of the executive authority, which may lead to delays in issuing the executive regulations and, consequently, the suspension of the law's enforcement. Therefore, referrals to the executive regulations should be limited to what is strictly necessary, including procedural details and precise technical aspects.

Limits on Power Delegation to Executive Entities

The law should grant the executive entities entrusted with enforcing its provisions sufficient authority to carry out their roles effectively. However, these entities should not be given discretionary powers that could compromise the consistent application of the law or infringe upon the judiciary's role.

Additionally, no executive entity should be granted blanket exemptions from compliance with the law regarding its use of AI. Any special considerations for such entities must be addressed through procedures that maintain the consistency of the law's application.

Key Principles for Ethical AI Governance

In January 2025, "*Masaar*" released a detailed paper titled "An Approach to AI Governance: Essential Frameworks for Promoting Justice and Protecting Human Rights." This paper includes an in-depth explanation of the fundamental principles required for the ethical governance of AI technology. Below are the principles discussed in the paper:

- Security, Transparency, Inclusivity, and Fairness.
- Proportionality, Continuous Learning, and Freedom of Expression.
- Capacity Building, Non-Discrimination, and Human Oversight.
- Redress and Remedy, International Cooperation, and Accountability.
- Ethical Considerations, Access to Justice, and Data Quality
- Avoiding Bias, Prohibition of Mass Surveillance, and Protection of Vulnerable Groups.
- Social and Environmental Responsibility and Human Rights Impact Assessments.
- Prohibition of Lethal Autonomous Weapons.
- Privacy and Data Protection, and Multi-Stakeholder Cooperation.
- Prevention of AI misuse, and Ethical Use of AI in Law Enforcement.

This paper uses these fundamental principles to derive criteria for assessing the extent to which the provisions of legislation regulating AI in Egypt align with them. On the other hand, the following sections of the paper organize the evaluation criteria to correspond as closely as possible to the expected structure of the law.

Therefore, each of the criteria outlined below may contribute to achieving one or more of the fundamental principles. Similarly, the tasks of fulfilling any of these principles may be distributed across multiple criteria belonging to different sections of the law. Nevertheless, the relationship between each criterion and the principles it aims to achieve will become clear in the discussion of each criterion individually.

Criteria for Evaluating the Provisions of the Law

This section, in its various parts, discusses detailed criteria for evaluating the provisions and texts of an Egyptian law regulating AI. These criteria are formulated based on the fundamental principles of ethical AI governance and international legislative experiences and guidelines previously mentioned. Finally, these criteria also depend on the prior local expertise in the legislative regulation of advanced technology fields, including both the positive and negative aspects of this experience.

General Provisions

Legal Jurisdiction and Scope of Application

Digital technology fields that rely on networks, primarily the Internet, are characterized by the fact that a significant portion of their applications transcend traditional legal jurisdiction. AI is no exception in this regard since many AI applications are available as digital services through the Internet.

This enables individuals and institutions to access them from anywhere in the world. Additionally, the processes of collecting, storing, and processing data used in developing and using AI systems are often transnational and distributed across data centers worldwide.

To address this issue, the law should adopt an approach based on defining its scope of application through the intersection of two domains:

- The scope of impact of the AI system.
- The scope of legislative responsibility for protecting the rights and interests of citizens and residents on Egyptian territory.

In other words, the scope of the law application should include any AI system in which any stage of its lifecycle takes place within Egypt's geographical borders. This includes usage stages that may occur through individuals and institutions accessing the AI system via the Internet.

Key Definitions

A previous section of the paper discussed several linguistic and drafting considerations related to the law's definition of the terms it contains. Furthermore, the following points present considerations specific to certain definitions of particular importance.

- **Definition of an AI System**: This definition is central to determining the scope of the law's application and identifying which types of software fall within its jurisdiction and are subject to its provisions. In practice, there are various types of AI, such as machine learning systems, deep learning systems, and others. Additionally, new AI technologies are likely to emerge soon. Therefore, while the definition of AI systems must encompass all current technologies, it should also be broad enough to include any future technologies that may arise shortly. This can be achieved by defining the AI system based on its distinguishing characteristic- its ability to simulate human cognitive processes in data processing, particularly in decision-making.
- **Risk-based Classification of AI Systems**: The law should provide clear definitions for AI systems with unacceptable risk, high risk, limited risk, and low risk. These definitions should reflect the classification criteria established by the law to differentiate between various levels of AI system risks. The paper discusses these criteria in detail in a later section.

- **Definition of Training and Testing Data**: The law should clearly define datasets explicitly used for training and testing AI systems. These datasets should be distinguished from other data that may be used as inputs to an AI system during its operational stages, as they are subject to special considerations outlined in the law's provisions.
- **Human Oversight:** The law should provide a clear definition of what is meant by effective human oversight. Such oversight is not limited to merely monitoring the performance of an AI system but must also include a sufficient degree of intervention capability, accompanied by human responsibility and accountability.

Classification of AI Practices and Systems

This section addresses the criteria for evaluating the law's classification of AI practices and products to achieve the risk-based approach of graduated requirements and obligations.

Classification Criteria

- The classification criteria must be clear and precisely defined in form. This means avoiding any ambiguous, vague, or overly broad language in stating these criteria. Additionally, references to well-known real-world examples should be included to provide further clarity on what the criteria apply to.
- The classification criteria must cover all aspects that influence the level of risk posed by an AI system. The most important of these aspects include:
- The purpose of the AI system and the field in which it will be used.
- The potential impacts of all processes related to the design, development, training, testing, deployment, operation, and use of the AI system on the fundamental rights and safety of individuals and relevant institutions. This includes protection from physical and psychological harm.
- The levels of transparency provided by the AI system and the possibility and extent of human oversight intervention at different stages of its operation.
- The quality of the data used by the AI system for training and testing purposes and the likelihood of bias in the data.

Prohibited Practices

Some AI system practices constitute a clear violation of fundamental rights and freedoms. Some other systems pose direct risks to individuals' and institutions' lives, safety, and interests. In

addition to the need for classification criteria establishing specific rules for prohibiting certain AI systems, the law must explicitly prohibit certain practices, including:

- **Behavioral Manipulation**: The use of AI to direct or modify the behavior of individuals should be prohibited. This violates their freedom of choice and can lead to significant harm at the individual, institutional, and even national security levels.
- **Social Scoring and Profiling:** The use of AI for evaluating and/or classifying individuals socially must be prohibited, particularly in creating social credit systems, criminal profiling, and risk assessment based on criteria that lead to discrimination.
- **Facial Recognition and Biometric Data Collection:** The use of facial recognition systems and identity tracking based on data collection must be prohibited unless governed by legitimate and justified legal controls within strict limits, as it constitutes a severe violation of the right to privacy.
- **Emotion Inference and Sensitive Data Estimation**: The use of AI to infer individuals' emotions or indirectly derive sensitive personal data should be prohibited, except in cases of medically justified necessity (such as diagnosing physical illnesses and mental disorders…etc.) and only within the limits of legality, informed consent, and prior awareness.
- **Mass Surveillance**: The law must explicitly prohibit the use of AI in mass surveillance operations and the random, large-scale intrusion into information systems owned by individuals or institutions.
- **Lethal Autonomous Weapons**: The law should explicitly stipulate the prohibition of the use of autonomous weapon systems that rely on AI to identify targets and make decisions to use lethal force without human oversight or intervention.

High-Risk Systems

The following considerations should be taken into account when classifying any AI system as high-risk, based on the previously mentioned aspects:

- **Purpose and Use**: The law should specify in its classification criteria certain fields where AI systems are considered high-risk. Examples of such fields include sensitive sectors like healthcare and security and decision-making systems that directly impact individuals' fundamental interests, such as loan approvals and eligibility for essential services.
- **Potential Impacts on Fundamental Rights and Safety**: The classification criteria must include an assessment of the likelihood that the system could violate human rights or pose risks to individuals' health and safety. AI systems whose use could restrict individuals' freedoms, discriminate against them, or harm public health or safety should be classified as high-risk. Clear limits for such potential risks must be specified, and relevant systems must be entirely prohibited.

- **Levels of Transparency and Human Oversight**: The classification criteria for AI systems should consider the level of human oversight and intervention different systems allow. Systems that do not meet a defined level of transparency and human oversight should be classified as high-risk, ensuring that stricter requirements and obligations are applied to them.
- **Data Quality and Potential Bias:** AI systems that are likely to rely on data with uncontrollable quality or inherent bias should be classified as high-risk. This classification allows for the enforcement of stricter obligations to detect poor data quality or biases.

Requirements for Approving AI Systems

Compliance Safeguards

The law should establish safeguards to ensure that entities responsible for developing, deploying, and using AI systems comply with the stipulated requirements. These safeguards should include:

- **Monitoring and Oversight Mechanisms**: The law should assign oversight responsibilities to one or more official bodies or establish a specialized authority to oversee the enforcement of its provisions. This body or bodies should monitor development and marketing processes and conduct periodic evaluations to ensure ongoing compliance.
- **Registration in Public Databases:** The law should mandate the establishment of a public database in which entities responsible for developing, deploying, and using high-risk AI systems must register these systems. This ensures transparency, facilitates tracking, and enables monitoring their impact on users.
- **Risk Assessment and Technical Documentation Procedures**: The law should obligate entities responsible for developing, deploying, and using AI systems to conduct comprehensive risk assessments as part of the documentation required for system approval. Additionally, these entities should be mandated to maintain detailed records, including information on training data, testing methods, and risk management mechanisms. This enables authorities to review performance and ensure systems comply with legal requirements.
- **Imposing Penalties and Financial Fines:** The law should stipulate appropriate penalties for violators. When determining penalties, consideration must be given to the actual or potential impact of the violation and the financial returns that constitute the motivation for committing it. Penalties can range from financial fines to the suspension or complete revocation of relevant approvals, licenses, and permits.

Crisis Management Systems

The law should include a definition of the concept of crises related to the development and use of AI. By way of enumeration, it should specify the cases that constitute a crisis requiring management through a special mechanism. Additionally, the law should specify the existing entities or those that are to be established based on its provisions, responsible for handling these crises.

Moreover, the law must stipulate the procedures to be followed for crisis management. This includes the methods for detecting or reporting a crisis threat or occurrence, the entities that must be notified, and the specified timeframe for doing so. The law should also define the various relevant entities' roles, obligations, and responsibilities.

Procedures to be stipulated regarding crisis management must include achieving transparency commensurate with the nature and scale of the crisis. This entails methods for informing concerned parties and potential victims, along with related timeframes and means for publicly announcing the crisis, its progression, and the actions taken to address it.

Data Governance

The provisions of the law related to data governance should take into account the following considerations:

- **Ensuring Data Quality and Relevance**: The quality and relevance conditions specifically pertain to the data used in training AI models. The law should mandate that the responsible entity provides necessary measures to verify the quality of this data (accuracy, comprehensiveness, representativeness, and lack of bias) and ensure its suitability for the intended purpose.
- **Applying the Principle of Data Minimization**: The law should mandate the responsible entity to provide evidence of compliance with the principle of data minimization. This means that, at any stage of AI development and use, the entity must not collect any data beyond what is necessary to achieve the system's intended purpose.
- **Mechanisms for Detecting Data Bias**: The law should mandate the responsible entity to provide evidence of implementing or incorporating mechanisms within the AI system that allow for the detection of any data bias during the system's development, training, or deployment phases.
- **Transparency and Documentation**: The law should mandate the responsible entity to provide all information clarifying the sources of data used in developing and using the AI system. It should also mandate the entity to document this data, maintain the documentation, and present it

to oversight and regulatory authorities in an appropriate format upon request in cases specified by the law.

- **Integration with the Risk Assessment Framework**: The procedures stipulated by the law regarding data governance must integrate with the risk assessment framework. The responsible entity's risk assessment report must evaluate the data sensitivity the system will use, potential data leakage or breach risks, and available security measures to prevent such incidents.

Documentation and Record-Keeping

Documentation is one of the fundamental pillars supporting the principle of transparency. It is also essential for enabling the monitoring, oversight, and supervision mechanisms required by the law as part of compliance safeguards. Several criteria include documentation requirements, which the paper has discussed when addressing these criteria. This section presents additional considerations, including:

- **Design and Development Documentation**: The law should mandate entities responsible for developing AI systems to prepare comprehensive technical documentation. This documentation should explain the system's internal design, training methods, and decision-making mechanisms, ensuring clarity in the development process and providing a technical reference for later use in assessing compliance with the law's requirements.
- **Documentation of Training and Testing Data:** Entities responsible for developing AI systems should be mandated to specify the sources of the data used, particularly the tests conducted to ensure data quality, diversity, and absence of bias. Additionally, they must describe the processes followed for data cleaning and encoding.
- **Records of Assessment and Risk Management**: The law should mandate entities responsible for developing high-risk classified AI systems to conduct periodic risk assessments, including analyzing the system's impact on fundamental rights and safety. These entities should also be mandated to document the results and corrective measures taken, with the stipulation that these records be made available upon request by the relevant oversight authorities.

Transparency Requirements

The law should mandate that the entity responsible for developing and deploying an AI system implement sufficient measures to meet transparency requirements. These requirements include those related to both data governance and documentation.

The law should also require entities responsible for developing and deploying AI systems that provide services directly to the public to publish, through easily accessible channels, sufficient information regarding the following:

- The type of data used by AI systems and how it is processed.
- Direct contact information for individuals who need to inquire whether their personal data is being collected and processed.
- Information on how individuals can exercise their right to modify, correct, or delete their personal data.

Transparency requirements also include mandating entities responsible for developing and deploying high-risk AI systems to publish periodic reports on the performance of these systems and any issues or threats they have encountered. Furthermore, they should be mandated to publish emergency reports in the event of a security incident that could result in harm to individuals or institutions.

On the other hand, the law should mandate that the relevant oversight, supervisory, and investigative authorities publish periodic reports on their activities and emergency reports on specific incidents. If the circumstances of any investigation necessitate non-disclosure during its course, the investigation's results should, in all cases, be made public.

Human Oversight

The law should impose requirements ensuring the availability of a minimum acceptable level of human oversight over AI systems during their development and use. The availability of human oversight should be considered as a factor in AI classification standards in terms of risk. Moreover, the requirements and obligations imposed by the law should take into account the following considerations to ensure an appropriate level of human oversight:

- **Real-Time or Live Human Oversight**: For sensitive and critical applications, such as public utilities or security systems, the law should require mandatory live human monitoring and oversight of AI system operations.
- **Human Responsibility for Decision-Making:** The law should require that AI systems making decisions that impact individuals' interests or pose potential threats to their rights be subject to review by human officials.
- **Human Intervention:** The law must require that high-risk AI systems allow human intervention to modify or halt their operation when necessary. It should also explicitly specify the

situations where such intervention is mandatory and outline the legal responsibilities resulting from its absence.

Accuracy, Quality, and Cybersecurity

The law should include provisions mandating that entities responsible for developing and deploying AI systems implement safeguards related to accuracy, quality, and cybersecurity considerations. These safeguards include:

- Mandating the submission of certified test results to evaluate the system's accuracy, particularly regarding its decision-making mechanisms.
- Mandating assessments of the system's relevance to its intended purpose and quality ensures it is free from critical defects, programming errors, or any issues in the information environment it relies on.
- Mandating proof of the system's compliance with cybersecurity considerations and the absence of vulnerabilities that could threaten its operation, the data it uses, or the information systems it operates on.

Obligations of High-Risk System Service Providers

The law should clearly distinguish between the general requirements and obligations that apply to all providers of AI system services and the additional requirements and obligations that apply only to systems classified as high-risk.

These considerations represent the minimum necessary requirements. However, the legislator may find it necessary to expand the obligations imposed on this type of system. The additional requirements should include data governance considerations, documentation, transparency, risk assessment, and human oversight and intervention.

Impact Assessment on Fundamental Rights

The law should stipulate a set of procedures that ensure the availability of an assessment of the potential impact of AI systems on fundamental human rights and freedoms. This assessment is one of the key tools for classifying AI systems based on their level of risk and determining the corresponding obligations necessary to safeguard rights and freedoms. In this context, the legal provisions must cover and address the following considerations:

- **Comprehensive Risk Assessment**: The law should mandate that system providers conduct a detailed assessment of the potential impacts of AI on fundamental rights. This includes privacy and data protection, fairness, non-discrimination, freedom of expression, and access to information. The law should also stipulate that this assessment covers all stages of the system's design, development, deployment, and use. Moreover, the law should require periodic updates to this assessment as the system evolves and its operating environment changes.
- **Precautionary Measures**: The law should impose additional obligations on providers of high-risk systems, particularly those potentially threatening fundamental freedoms and rights. These obligations relate to implementing risk mitigation measures and providing enhanced oversight of the system's operations. This includes guarantees to enhance transparency and ensure effective human oversight, with the ability to intervene in actual threats, bias, or system malfunctions.
- **Transparency and Accountability**: The law should mandate AI system providers to publish the impact assessment results and make them available to oversight authorities. Furthermore, the law should establish clear oversight, monitoring, and accountability procedures in cases of non-compliance or negligence leading to harm.
- **Integration with Risk and Crisis Management**: The law should mandate integrating AI system impact assessments on fundamental rights into the risk and crisis management framework. Impact assessments provide a key information resource for this framework and allow for identifying potential risk sources to anticipate the emergence and escalation of crises.

Requirements for Systems with Special Characteristics

The law must specify requirements tailored to the nature of certain AI systems with special characteristics. These systems are identified either due to the sensitivity of their application domain and/or the breadth of their impact or due to the sensitivity of the data they handle.

The law can stipulate special oversight and monitoring mechanisms for these systems and impose stricter procedures and obligations on their developers and users regarding documentation, human oversight and intervention, risk assessment reports, and other requirements.

Regulatory Procedures

Approval, Licensing, and Authorization Procedures

Approval, licensing, and authorization procedures are among the main pillars through which many of the law's objectives are achieved. These procedures ensure that AI systems meet the various requirements of the law. Given the importance of these procedures, the law's provisions related to them should be highly precise. Additionally, these provisions should consider a set of key considerations, including:

- Carefully determine which AI-related activities require long-term approval, renewable licenses for performing specific activities, or temporary or task-specific authorization.
- Given the nature of AI systems, licensing or authorization requirements can be highly complex. The documents required for submission and review are expected to be numerous and potentially extensive. Therefore, the law should account for this in the timelines it sets for submitting required documents, reviewing them, making decisions, and balancing the purpose of the review process with the interests of entities seeking licenses or authorizations.
- Procedural simplification should be considered during the review of licensing or authorization applications so that applicants only need to interact with a single central authority, which will internally distribute the review tasks.

Procedures of Oversight, Supervision, and Compliance with Law Requirements Assessment

Procedures of oversight, supervision, and compliance with law requirements assessment are directly linked to approval, licensing, and authorization processes, as they all share most of the law's provisions. In other words, the law defines the requirements on which approval, licensing, and authorization decisions are based, and these exact requirements form the foundation for oversight and supervision processes to ensure compliance with the law. This section addresses the general considerations for these procedures, the most important of which are:

- The law should ensure that oversight, supervision, and assessment procedures are only as intrusive as necessary to achieve their objectives without causing unjustified disruption to the processes they oversee.
- Oversight, supervision, and assessment procedures should be conducted periodically, with balanced time intervals. These intervals should not be too short, as this could hinder the continuity of the operations subject to oversight. Nor should they be too long, as this could delay the detection of issues or violations, potentially preventing timely intervention and resolution.
- Non-periodic oversight procedures should be justified by necessity. They should escalate their level of intervention into the processes being overseen based on the severity of the reasons that prompted them.

Investigation Procedures and Administrative Penalties

The law must explicitly specify the cases that necessitate administrative investigations. It should also define the investigating authority, its jurisdiction, and its powers in a manner that enables it to access the necessary information to verify allegations and determine responsibility.

Investigation procedures and the imposition of administrative penalties should ensure the following:

- The conditions that trigger an investigation must be unambiguous.
- The duration and timing of different procedures should be balanced, including the period between notification or reporting, the commencement of the investigation, information gathering from relevant entities, and the conclusion of the investigation with a final decision.
- Administrative penalties should be proportionate, including fines, suspension, or revocation of approvals, licenses, or operating permits.
- Mechanisms for appealing the decisions of the investigating authority during and after the investigation should be available.
- Procedures for notifying potentially affected individuals of any actual or potential harm (e.g., data breaches or leaks) and providing them with the necessary information to seek redress and/or appropriate compensation should be stipulated.

Criminalization Cases and Regulation of Criminal Penalties

The law should avoid any legislative duplication by criminalizing acts already punishable under existing laws. It must integrate with other laws by specifying any special procedures necessary for their enforcement, particularly regarding obtaining the information required to prove suspected facts related to the use of AI systems.

Otherwise, the task of criminalization and imposing criminal penalties is limited to acts exclusively related to the procedures of the law and not subject to criminalization under any other law. Examples include developing and using AI systems with unacceptable risk levels, which the law prohibits from being developed or used. The intended criminalization in this context includes developing and using such systems even if the potential harm has not been conclusively realized.

The law must stipulate that criminal penalties apply to the development and use of prohibited systems and any penalties imposed by other laws if actual harm whose criminalization falls under their jurisdiction occurs.

The law should also specify procedures for notifying individuals and entities proven to have been harmed by criminally punishable acts. This ensures their rights to pursue civil claims or other legal actions to redress the harm they have suffered and/or compensate them for it.

Harm Assessment, Redress, and Compensation Mechanisms

Law provisions should include establishing mechanisms and procedures to enable the following:

- A mechanism for reporting harm caused by using AI systems (directly or through a third party).
- Mechanisms for investigating reports and complaints and proving the occurrence of harm.
- Mechanisms for assessing proven harm, estimating possible redress measures, and determining compensation.
- Reporting procedures should not be overly complex. The complainant should have access to information proving the occurrence of harm, and the investigating authority must consider this information in addition to what it obtains independently.
- The complainant and the subject of the complaint should have access to mechanisms for appealing any decisions made during the investigation or determining redress and compensation measures.

Procedures to Support Development, Innovation, and Testing Capabilities

The law can support development, innovation, and testing capabilities through several means, including:

- **Balancing the Imposition of Requirements and Obligations in Favor of Small and Emerging Local Entities:** The law may stipulate exemptions for certain AI systems from some procedural requirements, provided that these systems are developed locally- especially by small or emerging entities, universities, or research centers.
- **Providing Risk Assessment Services:** The law may stipulate that relevant official bodies conduct risk assessments for AI systems developed by small, emerging, or research entities.
- **Providing Testing Environments**: The law may stipulate that the state establishes technical facilities, including testing environments for AI systems. Access to these environments may be provided for a fee proportional to the size of the entity developing the AI system, with the possibility of offering free access to startups and research institutions.

Procedures for Supporting International Cooperation

The law may promote international cooperation in the field of AI development and regulation through measures such as:

- **Ensuring Compatibility with International Legislations:** The law may allow local licensing and permitting authorities to recognize similar international licenses and permits for AI systems if the conditions for obtaining them are compatible with the requirements stipulated in Egyptian law.
- **Facilitations for International Cooperation Initiatives and Projects:** The law may provide procedural facilitations for AI systems developed through international cooperation initiatives and projects.
- **Cooperation in Investigations and Crisis Management:** The law should establish mechanisms for cooperation with external entities in investigating threats and violations arising from cross-border AI applications. Moreover, it should outline procedures for cooperation in managing cross-border crises related to AI systems.
- **Regulatory Procedures for State Institutions' Use of AI Systems:** The law may establish specific procedures for AI systems developed, deployed, or used by official state institutions or state-affiliated institutions. These procedures may impose additional requirements due to the sensitivity of the functions performed and/or the data used. They may also delegate oversight and supervision tasks to state-affiliated bodies, with guarantees for transparency and the right to access information.

Procedures for Regulating the Use of AI Systems by Law Enforcement and Security Agencies

The law should not grant any blanket exemptions from its requirements for AI systems developed or used by law enforcement and security agencies. Instead, the law can stipulate special procedures tailored to the nature of these systems, the data they use, and national security considerations. It must also emphasize sufficient safeguards, including judicial oversight of these procedures and guarantees for the right to access information for affected individuals, particularly in cases of criminal prosecution and trials.

Regulatory, Oversight, and Advisory Bodies

The Competent Authority: Purpose and Role

The law should establish a competent authority tasked with overseeing the implementation of its provisions. This authority's roles include issuing the approvals, licenses, and permits required by the law to develop, deploy, and use AI systems, ensuring compliance with the law's requirements. It is also responsible for supervising AI systems and conducting periodic monitoring to ensure their continued compliance with law requirements.

Functions, Powers, and Scope of the Competent Authority

The law must explicitly and clearly define, by way of enumeration, the functions of the competent authority and the details of its responsibilities. It should also specify the powers granted to this authority, strictly in line with the requirements for performing its assigned functions. Additionally, the law should clearly define the scope of this authority's jurisdiction, ensuring it does not overlap with the jurisdiction of other official bodies.

Structure and Composition of the Competent Authority

The special provisions of the law on the structure and composition of the competent authority should ensure that they are appropriate for its assigned functions and the expected volume of work. It must also ensure the availability of the necessary technical, financial, and human resources for the authority to fulfill its role. The composition should balance representation from state institutions, technical expertise bodies, and stakeholders.

Requirements for Independence, Transparency, and Accountability

The law must ensure that the competent authority has an appropriate level of independence from entities over which it may exercise oversight or supervisory functions. This includes official bodies, state institutions, and relevant private sector entities.

The law should also stipulate procedures to ensure transparency in the operations of the competent authority. It must mandate detailed documentation of its activities, the maintenance of comprehensive records, and the issuance of periodic reports covering its various activities. Finally, the law should clearly define the authority's responsibilities for the outcomes and impacts of its functions and mechanisms for monitoring its performance and holding its officials accountable.

Role of Advisory Bodies and Procedures for Accreditation and Registration

The law must regulate the roles that technical and advisory service providers related to AI and its systems can perform. These roles range from providing technical consultations to entities

developing and deploying AI systems to offering advice in cases of investigations and criminal trials, among others. The law should also stipulate procedures for accrediting these entities appropriately to their various roles.

Conclusion

This paper provided comprehensive and detailed criteria for evaluating legislation regulating AI technology in the Egyptian context. These criteria were formulated based on the fundamental principles of ethical AI governance, previous international legislative experiences, and Egypt's National AI Strategy.

The first section of the paper discussed the general frameworks for legislation regulating the use of AI in the Egyptian context. This section covered the relevant environments in which the law would be issued, as well as its philosophy, vision, objectives, and the optimal approaches it should adopt to achieve its intended purpose.

The second section discussed the general criteria for evaluating the legislation and the fundamental principles from which the detailed criteria are derived. Finally, the third section presented evaluation criteria for the specific provisions of the law, including general provisions and those related to requirements, obligations, and the various procedures that the law should regulate.