CLIENT UPDATE

IN READINESS FOR THE USE OF AI, PART 2: MANAGING CYBERSECURITY RISKS

Background

Mexico is keeping track of the approval process of the European Union Artificial Intelligence Act (the "EU AI Act") , and it is likely to model a new statute that will consider such Act as guidance.

In Part 1 of this Berdeja Update series, we address the EU AI Act coverage of the state of AI regulation and best practices recommendations for AI risk management and governance.

Part 2 will cover the EU AI Act assessment of uses of AI in cybersecurity and fraud protection, and opportunities for readiness by Mexican corporations, that will make it easier to implement a future statute governing AI in Mexico.

EU AI Act

As discussed in our previous Update here, the EU Artificial Intelligence Act was adopted on March 13, 2024 and it will go into effect twenty days after its publication in the EU Official Journal. In parallel to AI prescribed practices and controls, the Act mandates implementation of cybersecurity measures to ensure a safe and secure use of them.

The EU AI Act establishes that:

(a) Providers of general AI models with systemic risk shall ensure an adequate level of cybersecurity protection for the general-purpose AI model with systemic risk and the physical infrastructure of the model;

(b) Providers shall furnish instructions of use to deployers that inform the level of accuracy, including its metrics, robustness and cybersecurity against which a high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity.

Preparation for Cybersecurity Measures

Companies should spend time and effort now, preparing for cybersecurity measures to be adopted, focusing on managing operational risk.

The following aspects should be considered.

- Cyberattacks Enhanced with AI.
- Malware/Code generation and automated discovery of vulnerabilities.
- Disinformation using AI.
- Data poisoning.
- Data leakage during inference.
- Evasion.
- Model extraction.

Firms should consider controls that will support secure deployment and in-production use of AI systems. Firms may want to have defined cybersecurity expectations for AI systems that are appropriate to risks of the system, such as having appropriate access controls, a segregated environment that holds golden-copies of code, as well as verification requirements, and keeping of earlier versions of AI models should the newest version be misused or compromised.

Companies are likely to be made subject to specific rules issued by Mexican regulators. However, the above-mentioned suggested preparatory steps, are likely to put them in the front row of the starting line, when such rules are issued.

* * *

Please do not hesitate to contact us with any questions.

Berdeja Abogados, S.C.

July 23, 2024