From autonomy to centralization: Rethinking data protection oversight in Mexico

Daniela Márquez-Ledezma

On March 20, 2025, the Mexican Federal Congress approved a package of reforms that included, among others, the enactment of a new Federal Law on the Protection of Personal Data Held by Private Parties, and a corresponding law for public entities. The reform, promoted by the outgoing president and the ruling political party, has sparked significant debate within legal and data protection circles. Critics argue that it represents a step backward in Mexico's regulatory progress on privacy and transparency.[1]

This article aims to provide a legal analysis—while avoiding political bias—of the key changes introduced by this reform, and their potential implications for private companies and individuals in an increasingly global and data-driven economy.

General overview

While the reform appears to draw inspiration from the EU's General Data Protection Regulation (GDPR), several provisions fail to align with Mexico's social and institutional reality. In particular, awareness of data protection and transparency rights remains limited across large segments of the population. By virtue of this reform, all secondary legislation was repealed and its publication in the Official Gazette is still pending.

The elimination of INAI

Arguably the most significant change is the dissolution of the National Institute for Transparency, Access to Information and Protection of Personal Data (INAI). This autonomous constitutional body, independent from all branches of government, was responsible for supervising, sanctioning, and promoting the enforcement of data protection and access rights.

These powers are now transferred to the newly created Secretariat for Anti-Corruption and Good Governance. Unlike INAI, this body is part of the federal executive, raising concerns about independence and impartiality. Among INAI's most valued roles was its public outreach work—promoting awareness of ARCO rights (Access, Rectification, Cancellation, and Opposition) and empowering individuals to exercise them.

Redefining the object of protection

Another major shift is the removal of the term "physical" from the definition of personal data. The law now defines personal data as "any information concerning an identified or identifiable person," without limiting it to natural persons.

This change opens the door to interpreting that legal entities could also be protected under the law, which would deviate from the established principle that personal data is intrinsically

[1] R3D: Red en Defensa de los Derechos Digitales. (2025, March 21). *Las nuevas leyes de transparencia y protección de datos personales: Retrocesos y oportunidades perdidas*. https://r3d.mx/2025/03/21/las-nuevas-leyes-de-transparencia-y-proteccion-de-datos-personales-retrocesos-y-oportunidades-perdidas/

linked to human dignity, autonomy, and identity. The risk is that extending protection to legal entities could dilute the focus on individuals' rights, potentially allowing misuse by entities seeking to shield corporate information under the guise of personal data.

Broader definitions and stricter requirements

- **Expanded definition of processing**: The concept now includes any manual or automated action performed on personal data, from collection to deletion.
- **Binding self-regulation**: Companies may adopt internal codes of conduct or compliance models, which can be registered with and monitored by the Secretariat.
- **New privacy notice standards**: Data controllers must clearly inform individuals of the exact purpose and scope of data processing.
- **End of broad consent**: The prior allowance for using data for "compatible purposes" has been removed. Processing must now be directly related to the specified purpose.
- **Minimum retention**: Controllers must ensure that data is only processed for as long as strictly necessary.
- **Confidentiality with systemic controls**: Unlike the previous law, which required confidentiality on an individual level, the new law mandates structural mechanisms and controls throughout all stages of processing.

The creation of specialized courts

The reform mandates the creation of specialized courts to handle data protection and access to information matters. These courts must be established within 120 days from March 21, 2025.

This change has been criticized for transferring sensitive decisions to judges who may lack subject-matter expertise. Unlike INAI's administrative procedures, individuals will now need to initiate full legal proceedings, potentially via amparo, increasing the burden on those seeking to enforce their rights.

Compounding the issue is the judiciary reform introduced by the same administration, which proposes replacing current judges through popular elections—a move that raises serious concerns about judicial independence.

Automated processing and digital identity

The new law allows individuals to object to or demand cessation of automated processing when it produces legal effects or significantly affects their rights and freedoms without human intervention.

In a world dominated by big data, artificial intelligence, and massive digital ecosystems, this provision acknowledges the need for human oversight in algorithmic decision-making. However, it also underscores the urgency of developing clear rules and institutional capacities to protect our digital identities, especially for vulnerable groups like children and adolescents.

Final reflections

From a legal perspective, the reform introduces both progress and risk. While it aligns certain standards with international practices, it also centralizes control, eliminates an autonomous oversight body, and introduces ambiguities that may hinder the effective protection of personal data.

Given the new enforcement framework, it is essential for private-sector organizations to carefully assess their compliance with the updated law and remain attentive to how the new Secretariat for Anti-Corruption and Good Governance will interpret and apply its sanctioning powers. In this transitional period, companies should adopt a proactive compliance strategy, reinforce their internal privacy controls, and seek legal guidance to navigate an evolving—and potentially more politicized—regulatory environment.