ECIJA MÉXICO

INSIGHT
August 3, 2026

LABOR / INTELLECTUAL PROPERTY

The Artificial Intelligence Prompt as a Potential Vehicle for the Disclosure of Trade Secrets under Mexican Law

IN BRIEF

The widespread use of generative artificial intelligence tools in the workplace has given rise to a legal risk that, until only a few years ago, was virtually nonexistent: the possibility that an employee, by drafting a simple message or prompt addressed to an AI system, may disclose or make the company's confidential information available to a third party outside the employment relationship. This article examines whether such conduct may constitute a violation of trade secret protections under Mexican law, as well as the specific consequences it may entail in the employment context. The issue is far from merely theoretical. Today, employees in areas such as engineering, finance, marketing, and software development routinely rely on AI assistants to generate code, summarize contracts, analyze databases, or prepare proposals, often without realizing that the information they input into such tools may be legally protected as a trade secret.

The Federal Law for the Protection of Industrial Property (Ley Federal de Protección a la Propiedad Industrial, or "LFPPI"), in force since November 5, 2020, regulates trade secrets under Title Twelve. Article 163, Section I, defines a trade secret as information of an industrial or commercial nature that a person maintains as confidential and that provides a competitive or economic advantage over third parties. However, the law does not protect any information that a company merely intends to keep confidential. For such protection to apply, the owner must have adopted sufficient measures or systems to preserve its confidentiality and restrict access to it.

This requirement has a particularly significant practical consequence for the matter at hand: trade secret status is not an inherent or permanent characteristic of the information, but rather a legal status whose preservation depends on the existence and continued implementation of reasonable protective measures. When those measures are compromised—for example, when the information is transferred from the company's controlled environment to an external platform—the owner risks losing the corresponding legal protection, even if the information was never intended to be disclosed.

Article 163(II) also defines misappropriation as the acquisition, use, or disclosure of a trade secret in a manner contrary to honest practices and customs in industry, commerce, and services, when such conduct entails unfair competition. Depending on who commits the act and for what purpose, the law provides for administrative and civil sanctions (including damages), and even criminal penalties.

There is not yet specific Mexican case law addressing the use of generative artificial intelligence and trade secrets; accordingly, the analysis must be based on the general principles of the LFPPI. Legally, the relevant issue is not the channel used—an email, a physical document, or an AI prompt—but whether the information left the control of the party protecting it and became accessible to a third party without adequate confidentiality safeguards.

Under this reasoning, uploading confidential information to an AI tool may amount to disclosure in any of the following circumstances: the service provider retains or uses the data to train its models; the service agreement or terms of use permit human review of the submitted content; the information is stored on servers outside the company's control and security measures; or unauthorized third parties gain access to the data through a breach or security incident affecting the provider. In any of these scenarios, the information is no longer under the exclusive control of the party that protected it—precisely the element Article 163 requires for legal protection to continue.

Nevertheless, a distinction should be drawn between AI tools with enterprise configurations that guarantee data will not be used for training or shared with third parties, and consumer-grade tools that lack such contractual safeguards. The existence of a confidentiality or data-processing agreement between the company and the AI provider may determine whether a legally relevant disclosure has occurred.

The Federal Labor Law (Ley Federal del Trabajo, "LFT") addresses this issue directly through two key provisions.

Article 134(XIII) establishes a general obligation for employees to strictly safeguard the technical, commercial, and manufacturing secrets of products in whose production they participate, directly or indirectly, or of which they become aware by reason of their work, as well as confidential administrative matters whose disclosure could cause harm to the company.

Article 47(IX), in turn, provides that an employee's disclosure of manufacturing secrets or confidential matters, to the detriment of the company, constitutes grounds for termination of the employment relationship without liability to the employer. Accordingly, if an employee enters company confidential information—such as formulas, production processes, source code, customer lists, business strategies, or non-public financial data—into a prompt addressed to an AI tool, and that conduct causes or is capable of causing harm to the company, it may, strictly speaking, constitute grounds for dismissal for cause, without any obligation to pay severance to the employee.

It is important to emphasize that the statute does not require malicious intent or bad faith on the part of the employee. It is sufficient to establish the disclosure of confidential information and the actual or potential harm resulting from it. Thus, an employee who uses an AI tool in good faith solely to work more efficiently may nevertheless be subject to dismissal for cause if the information shared was confidential and the employer can establish the resulting harm.

The foregoing gives rise to practical implications for both employers and employees. Companies should have a clear internal policy governing the use of artificial intelligence tools, defining the types of information that may and may not be entered into such systems, and incorporating that policy into the Code of Conduct and the Internal Work Regulations. Such a policy not only helps prevent information leaks but also facilitates establishing, in the event of noncompliance, the grounds for termination set out in Article 47(IX) of the LFT by showing that the employee was aware of the prohibition and knowingly violated it.

Companies should also assess the terms of service and privacy settings of the AI tools they authorize for internal use, prioritizing those that provide contractual assurances that submitted data will neither be used to train models nor shared with third parties. Supplementing these measures with robust confidentiality provisions in employment agreements strengthens legal protection and, in addition to employment remedies, may support a civil claim for damages under the LFPPI.

For employees, the principal recommendation is caution: when in doubt as to whether certain information constitutes a trade secret or a confidential matter, the safest course is to refrain from entering it into any external tool and to consult the relevant company department beforehand.

We may therefore conclude that a prompt submitted to an artificial intelligence tool is not, in itself, a legally distinct instrument from any other communication channel. What matters is whether it causes confidential information protected as a trade secret to leave the control of its holder and reach a third party without adequate safeguards.

When this occurs in an employment relationship, the LFT provides a clear answer: under Article 47(IX), read together with the confidentiality obligation under Article 134(XIII), an employee who discloses manufacturing secrets or confidential matters and thereby harms the company may have the employment relationship terminated without liability to the employer. The speed with which these tools have been adopted in Mexican workplaces requires both employers and employees to update their information-handling practices, because the existing legal framework—although not designed with artificial intelligence in mind—is fully applicable to the risks it creates.

CONTACTS

Tania Ávila
Partner
tavila@ecija.com

Miguel Angel Carpio
Partner
macarpio@ecija.com

Labor / Intellectual Property · info@ecija.com · T +52 55 5662 6840