

— LABORAL / PROPIEDAD INTELECTUAL

El prompt de inteligencia artificial como posible vehículo de divulgación de secretos industriales en el derecho mexicano

EN RESUMEN



El uso generalizado de herramientas de inteligencia artificial generativa en el entorno laboral ha dado lugar a un riesgo jurídico que, hasta hace pocos años, era prácticamente inexistente: que un trabajador, al redactar un simple mensaje o *prompt* dirigido a un sistema de IA, divulgue o ponga información confidencial de la empresa a disposición de un tercero ajeno a la relación laboral. Este ensayo analiza si dicha conducta puede constituir una violación de secretos industriales conforme a la legislación mexicana, así como las consecuencias que puede generar específicamente en el ámbito laboral. La cuestión dista de ser meramente teórica. En la actualidad, empleados de áreas como ingeniería, finanzas, mercadotecnia o desarrollo de software recurren cotidianamente a asistentes de IA para generar código, resumir contratos, analizar bases de datos o preparar propuestas, muchas veces sin advertir que la información que introducen en dichas herramientas puede estar jurídicamente protegida como secreto industrial.

La Ley Federal de Protección a la Propiedad Industrial (LFPPI), vigente desde el 5 de noviembre de 2020, regula la figura del secreto industrial en su Título Décimo Segundo. El artículo 163, fracción I, lo define como aquella información de aplicación industrial o comercial que una persona conserva con carácter confidencial y que le representa una ventaja competitiva o económica frente a terceros. Sin embargo, la ley no protege cualquier información que una empresa pretenda mantener en reserva. Para que dicha protección resulte aplicable, es indispensable que su titular haya adoptado medios o sistemas suficientes para preservar su confidencialidad y restringir el acceso a ella.

Esta exigencia tiene una consecuencia práctica especialmente relevante para el tema que nos ocupa: el carácter de secreto industrial no constituye una cualidad permanente de la información, sino un estatus jurídico cuya conservación depende de la existencia y continuidad de medidas razonables de protección. Cuando dichas medidas se vulneran —por ejemplo, al trasladarse la información desde el entorno controlado de la empresa hacia una plataforma externa—, su titular corre el riesgo de perder la protección legal correspondiente, aun cuando nunca haya tenido la intención de divulgarla.

El mismo artículo 163, en su fracción II, define la apropiación indebida como la adquisición, uso o divulgación de un secreto industrial de manera contraria a los buenos usos y costumbres en la industria, el comercio y los servicios, cuando ello implique competencia desleal. La ley contempla para estas conductas sanciones administrativas, civiles (indemnización por daños y perjuicios) e incluso penales, dependiendo de quién comete el acto y con qué finalidad.

No existe todavía jurisprudencia mexicana específica sobre el uso de inteligencia artificial generativa y secretos industriales, por lo que el análisis debe partir de los principios generales de la LFPPI. Lo jurídicamente relevante no es el medio empleado —un correo electrónico, un documento físico o un prompt de IA— sino si la información salió del control de quien la protegía y quedó al alcance de un tercero sin las garantías de confidencialidad adecuadas.

Bajo esta lógica, cargar información confidencial en una herramienta de IA puede equivaler a una divulgación cuando concurre alguno de los siguientes supuestos: que el proveedor del servicio conserve o utilice esos datos para entrenar sus modelos; que el contrato de servicio o los términos de uso permitan la revisión humana del contenido ingresado; que la información quede almacenada en servidores fuera del control y de las medidas de seguridad de la empresa; o que, por una filtración o incidente de seguridad del propio proveedor, terceros ajenos accedan a los datos. En cualquiera de estos escenarios, la información deja de estar bajo el control exclusivo de quien la protegía, que es precisamente el elemento que el artículo 163 exige para que subsista la protección legal.

Cabe distinguir, no obstante, entre el uso de herramientas de IA con configuraciones empresariales que garantizan que los datos no se usan para entrenamiento ni se comparten con terceros, y el uso de herramientas de consumo general sin dichas garantías contractuales.

La existencia de un acuerdo de confidencialidad o de procesamiento de datos entre la empresa y el proveedor de IA puede ser el factor que determine si hubo o no una divulgación jurídicamente relevante.

La Ley Federal del Trabajo (LFT) aborda este tema de manera directa, con dos disposiciones centrales. El artículo 134, fracción XIII, establece como obligación general del trabajador guardar escrupulosamente los secretos técnicos, comerciales y de fabricación de los productos en cuya elaboración participe, directa o indirectamente, o de los cuales tenga conocimiento por razón de su trabajo, así como los asuntos administrativos de carácter reservado cuya divulgación pueda causar perjuicios a la empresa.

Por su parte, el artículo 47, fracción IX, de la misma ley establece como causa de rescisión de la relación laboral, sin responsabilidad para el patrón, el que el trabajador revele secretos de fabricación o dé a conocer asuntos de carácter reservado, con perjuicio de la empresa. Esto significa que, si un trabajador introduce información confidencial de la empresa —fórmulas, procesos productivos, código fuente, bases de clientes, estrategias comerciales o datos financieros no públicos— en un prompt dirigido a una herramienta de IA, y esa conducta causa o es susceptible de causar un perjuicio a la empresa, en estricto sentido se actualiza una causal de despido justificado sin obligación de indemnizar al trabajador.

Es importante subrayar que la norma no exige que exista una intención dolosa o malintencionada por parte del trabajador. Basta con que se acredite la divulgación de la información reservada y el perjuicio, real o potencial, que de ella se deriva. Esto implica que un empleado que utilice una herramienta de IA de buena fe, únicamente buscando agilizar su trabajo, puede de cualquier forma incurrir en la causal de despido si la información compartida tenía carácter confidencial y su empleador puede demostrar el daño correspondiente.

De lo anterior se desprenden implicaciones prácticas tanto para empleadores como para trabajadores. Para las empresas, resulta indispensable contar con una política interna clara sobre el uso de herramientas de inteligencia artificial, que defina qué tipo de información puede o no introducirse en dichos sistemas, y que forme parte del Código de Conducta y del reglamento interior de trabajo. La existencia de esta política no solo previene fugas de información, sino que facilita, en caso de incumplimiento, acreditar la causal de rescisión prevista en el artículo 47, fracción IX de la LFT, al demostrar que el trabajador conocía la prohibición y la violó de manera consciente.

Asimismo, es recomendable que las empresas evalúen los términos de servicio y las configuraciones de privacidad de las herramientas de IA que autorizan internamente, privilegiando aquellas que ofrezcan garantías contractuales de que los datos ingresados no serán utilizados para entrenar modelos ni compartidos con terceros. Complementar esto con cláusulas de confidencialidad robustas en los contratos laborales refuerza la protección legal y habilita, además de la vía laboral, la posibilidad de reclamar daños y perjuicios por la vía civil conforme a la LFPPI.

Para los trabajadores, la recomendación central es la prudencia: ante la duda sobre si cierta información constituye un secreto industrial o un asunto reservado, lo más seguro es abstenerse de introducirla en cualquier herramienta externa, y consultar previamente con el área correspondiente de la empresa.

Podemos concluir que el prompt de una herramienta de inteligencia artificial no es, en sí mismo, un instrumento jurídicamente distinto a cualquier otro canal de comunicación; lo relevante es si, a través de él, información confidencial protegida como secreto industrial sale del control de su titular y llega a un tercero sin las garantías adecuadas. Cuando esto ocurre en el contexto de una relación laboral, la LFT ofrece una respuesta clara: el trabajador que revele secretos de fabricación o asuntos reservados, causando perjuicio a la empresa, incurre en una causal de rescisión sin responsabilidad patronal, conforme al artículo 47, fracción IX, en relación con la obligación de confidencialidad prevista en el artículo 134, fracción XIII. La rapidez con la que se han adoptado estas herramientas en el entorno de trabajo mexicano exige que tanto empleadores como trabajadores actualicen sus prácticas de manejo de información, pues el marco legal existente, aunque no fue diseñado pensando en la inteligencia artificial, resulta plenamente aplicable a los riesgos que ésta genera.

CONTACTOS



Tania Ávila

Socia

tavila@ecija.com



Miguel Angel Carpio

Socio

macarpio@ecija.com

Laboral / Propiedad Intelectual · info@ecija.com · T +52 55 5662 6840

La información contenida en este Client Alert es de carácter general y meramente informativa. No constituye asesoría legal sobre asuntos específicos y no debe utilizarse como sustituto de la consulta con un asesor legal calificado. Para asuntos específicos, le invitamos a contactar a nuestros profesionales.