# *De la confidencialidad analógica a la digital: retos y propuestas para regular el uso de tecnologías en instrumentos jurídicos, y velar por el deber de custodia*

**Alonso Gabriel Flores Delgado***

RVDM, nro. XV, 2025, pp. 479-499

**Resumen:** En la era de la transformación digital y la inteligencia artificial (IA), las prácticas tradicionales de confidencialidad y ética empresarial requieren actualización pues deben ajustarse a los cambios constantes, y a veces abruptos, del mercado. Los códigos de ética corporativos y los acuerdos de confidencialidad (NDA) deben contemplar expresamente el uso de herramientas de IA generativa, plataformas de traducción automática o servicios de conversión de archivos pues, de lo contrario, existe un riesgo creciente de filtración de información sensible. Este artículo revisa cómo adaptar esos contratos y códigos de conducta: ampliar la definición de "información confidencial" para incluir datos o *prompts* usados en IA, prohibir sin autorización el uso de herramientas externas no seguras y exigir entornos controlados (versiones empresariales o servidores propios) para procesar datos sensibles.

**Palabras clave:** ética corporativa, inteligencia artificial, confidencialidad, tecnología.

## *From analog confidentiality to digital: challenges and proposals for regulating the use of technologies in legal instruments and ensuring the duty of custody*

*Abstract: In the era of digital transformation and artificial intelligence (AI), traditional practices of confidentiality and business ethics require updating, as they must adapt to the constant—and sometimes abrupt—changes in the market. Corporate codes of ethics and non-disclosure agreements (NDAs) should explicitly address the use of generative AI tools, machine translation platforms, or file conversion services; otherwise, there is an increasing risk of sensitive information leaks. This article examines how to adapt these contracts and codes of conduct: Expand the definition of "confidential information" to include data or prompts used in AI, prohibit the use of insecure external tools without prior authorization, and require controlled environments (enterprise versions or proprietary servers) for processing sensitive data.*

***Keywords:*** *corporate ethics, artificial intelligence, confidentiality, technology.*

**Recibido:** 24/11/2025
**Aprobado:** 25/11/2025

* Abogado de la Universidad Central de Venezuela. Especialista en Derecho corporativo, Universidad Metropolitana, 2024. Email:alongabrielflores@gmail.com

# *De la confidencialidad analógica a la digital: retos y propuestas para regular el uso de tecnologías en instrumentos jurídicos, y velar por el deber de custodia*

**Alonso Gabriel Flores Delgado***

RVDM, nro. XV, 2025, pp. 479-499

## SUMARIO:



## INTRODUCCIÓN

La adopción masiva de tecnologías de Inteligencia Artificial (en lo adelante "IA") y herramientas digitales, cambia radicalmente la forma en que se maneja la información en las empresas, pues históricamente, los acuerdos de confidencialidad (NDA) protegían la información sensible compartida entre personas y estaban pensados para escenarios tradicionales de intercambio de datos. Sin embargo, hoy es común que empleados, colaboradores o proveedores ingresen directamente datos estratégicos a plataformas de IA generativa (como ChatGPT, Copilot o Google Gemini), o utilicen servicios de traducción en la nube y conversores de archivos online sin ser plenamente conscientes de los riesgos.

Estas acciones exponen en plataformas externas cualquier información confidencial, que podría almacenarse, reutilizarse o filtrarse[1] y, en la práctica, ello ha dado lugar

* Abogado de la Universidad Central de Venezuela. Especialista en Derecho corporativo, Universidad Metropolitana, 2024. Email:alongabrielflores@gmail.com

1 Blog de "eDefense" disponible en: https://edefense.es/https-edefense-es-blog-nda-ia-generativa-informacion/#:~:text=Hoy%20es%20habitual%20que%3A. En esta oportunidad, su equipo de trabajo explica que "El problema es evidente: si no adaptas tu NDA a la era de la inteligencia artificial, podrías estar dejando vacíos legales que comprometen tu know-how, tus ideas de negocio o incluso la información personal de terceros."

a incidentes reales: en 2023 varias empresas prohibieron ChatGPT tras descubrir que personal había subido código fuente sensible a la herramienta.

Un problema fundamental es que la confidencialidad en el mundo digital no está garantizada de forma automática; en la era analógica confiábamos en el secreto profesional y en que los sistemas de NDA abarcaban las comunicaciones entre individuos, pero como advierten recientes análisis legales, introducir información confidencial en sistemas de IA públicos no convierte automáticamente sus datos en confidenciales en el sentido legal.[2]

Dicho en otras palabras: ChatGPT y herramientas similares no ofrecen privilegios legales de secreto; los datos ingresados pueden ser almacenados, procesados o utilizados para entrenar el modelo, motivo por el cual los expertos británicos inciden que no debe considerarse a ChatGPT (o cualquier servicio de IA público) como una bóveda confidencial para secretos empresariales. En concreto, introducir información sensible o secretos comerciales en una IA pública puede anular la protección confidencial que se tenía, pues la IA podría "repetir" u "ofrecer" esos datos en consultas posteriores[3].

Estos hechos demuestran que el alcance de la confidencialidad contractual debe redefinirse, modificarse, y alinearse con la conducta de los colaboradores modernos. Es así que, si un NDA no contempla expresamente estos nuevos usos, surgen vacíos legales: el momento de "compartir" ya no es sólo al entregar un documento a un tercero, sino incluso al teclearlo en un chat automatizado[4], tomando en consideración que muchos NDA tradicionales ni siquiera contemplan el escenario de teclear o copiar/pegar material confidencial en un sistema automatizado externo. Los NDAs de antaño se fundamentan o están centrados en el intercambio humano de información (bien sea entregado entre manos, o a través de correos), pero dejan de lado el riesgo real de la transformación digital de datos.

---

[2] Alex Solo, en el artículo "Is ChatGPT Confidential? Understanding the Legal Implications and Privacy Considerations for UK Businesses", de fecha septiembre 2025, disponible en: https://sprintlaw.co.uk/articles/is-chatgpt-confidential-understanding-the-legal-implications-and-privacy-considerations-for-uk-businesses/ explica que "*Whether you're a founder, small business owner, or decision-maker at a growing company, it's worth pausing before you upload sensitive data, trade secrets, or client information to any AI system. Understanding the privacy and legal risks is crucial, so that your business stays protected from day one-no AI headaches down the line."*

[3] *"When you enter information into ChatGPT, it can be processed, stored, and-depending on your settings-potentially used to improve the AI model itself."* Alex Solo

[4] Simon Hodgkins, Confidentiality in the Age of AI: Why Your NDAs Probably Require an Upgrade. Disponible en: https://simonhodgkins.medium.com/confidentiality-in-the-age-of-ai-28d0d2a1e602

## *1. Códigos de ética, una perspectiva actualizada*

Un código de ética corporativo es un instrumento normativo interno que recoge los valores, principios y directrices que orientan el comportamiento de los miembros de una organización cuyo propósito es establecer un marco ético más allá del cumplimiento legal mínimo, proporcionando una guía coherente con la misión y visión institucional. El código de ética constituye una herramienta estratégica que refleja el compromiso organizacional con principios de integridad, equidad y responsabilidad. Su eficacia depende no solo de su contenido, sino también de su integración con las prácticas de gestión corporativa.

No se trata de una simple declaración de intenciones ya que, en entornos regulados, los códigos éticos integran el programa de cumplimiento de la empresa, siendo exigidos en licitaciones públicas, procesos de certificación y auditorías corporativas. Su adopción también es frecuente en organizaciones no empresariales como universidades, ONG, entidades financieras y organismos públicos, que lo utilizan como mecanismo de gobernanza interna.

Por lo tanto, desde una perspectiva jurídica y funcional, los códigos de ética cumplen al menos cuatro (04) roles:

- Normativo, al establecer los comportamientos aceptables e inaceptables;
- Preventivo, como mecanismo de mitigación de riesgos legales o reputacionales;
- Formativo, al orientar y educar a los colaboradores;
- Demostrativo, al permitir a la organización probar su diligencia frente a autoridades o socios.

Entonces, estos códigos funcionan como declaraciones de propósito que sirven tanto de guía interna como de escudo externo frente a potenciales acusaciones de negligencia organizacional. En América Latina, esta visión ha sido adoptada progresivamente, como lo muestra el análisis pues pueden ser valorados como prueba indirecta de la diligencia debida en investigaciones administrativas, penales o laborales[5], y aunque los códigos de ética no son leyes ni contratos en sentido estricto, su valor jurídico en procedimientos judiciales o administrativos ha ido en aumento, manifestándose en:

- Litigios laborales, donde la empresa busca justificar despidos por conductas contrarias al código.

[5] César Rojas López-Villalta, Ética empresarial y responsabilidad legal: fundamentos para la implementación de programas de cumplimiento (Bogotá: Universidad del Rosario, 2020), 78.

- Procesos penales contra directivos o la persona jurídica, donde se evalúa si existía un programa de cumplimiento eficaz.
- Controversias comerciales o de responsabilidad civil, donde se discute si la empresa fue diligente en prevenir daños.
- Investigaciones por autoridades regulatorias o fiscales, como evidencia de un entorno de integridad.

La OCDE[6], en su Good Practice Guidance on Internal Controls, Ethics, and Compliance, sostiene que los códigos éticos y los sistemas de cumplimiento son factores atenuantes clave para evaluar la responsabilidad empresarial en casos de corrupción, soborno o deficiencias internas, por lo que es preocupante que a pesar de su valor normativo e importancia, muchos códigos de ética conservan una visión analógica que omite desafíos modernos como la inteligencia artificial, el big data, el uso de plataformas externas no controladas, o la ingeniería inversa digital.

Se advierte que los códigos deben evolucionar desde herramientas formales hacia instrumentos adaptativos que consideren los riesgos emergentes de la inteligencia artificial y la automatización de decisiones[7], una visión que coincide con la tendencia observada en Asia, pues en Japón algunos códigos de ética corporativa ya incluyen "cláusulas específicas sobre IA generativa, protección de datos sensibles y transparencia algorítmica", integrando principios de gobernanza tecnológica como parte de la ética empresarial.

Es así que una actualización eficaz debe contemplar cláusulas sobre:

- El uso aceptado o prohibido de plataformas de IA generativa.
- El tratamiento de *prompts*[8] y resultados como información sensible.
- El uso de servicios de traducción automática, transcripción o conversión de documentos.
- La prohibición o regulación razonada de la ingeniería inversa sobre datos u operaciones.
- La integración con políticas de seguridad, confidencialidad y propiedad intelectual.

---

6 OECD, *Good Practice Guidance on Internal Controls, Ethics, and Compliance* (París: OECD Publishing, 2010)

7 Sophie Duroy, *Corporate Codes of Ethics in the Age of Artificial Intelligence: Between Compliance and Risk Governance, European Journal of Risk Regulation* 12, no. 3 (2021). La autora argumenta que los códigos deben "evolucionar desde herramientas formales hacia instrumentos adaptativos que consideren los riesgos emergentes de la inteligencia artificial y la automatización de decisiones.

8 Un *prompt* es el texto que se introduce para guiar la respuesta, el tono, el estilo o la tarea que debe ejecutar la IA.

- Adaptar los códigos de ética al contexto digital no implica restringir la innovación, sino enmarcarla bajo principios claros de responsabilidad, transparencia y diligencia.

## *2. Contratos de confidencialidad o Non-disclosure agreements (NDA) y deber de custodia*

Es un instrumento jurídico mediante el cual las partes se obligan a no divulgar ni utilizar indebidamente determinada información sensible o estratégica cuya finalidad es proteger los activos intangibles más valiosos de una empresa o individuo: conocimientos técnicos, planes de negocios, bases de datos, estrategias comerciales, algoritmos, entre otros. Son mecanismos contractuales que garantizan un entorno de intercambio controlado de información, fomentando la cooperación sin renunciar a la protección de la innovación o del secreto empresarial[9], sumamente habituales en relaciones laborales, negociaciones entre compañías, procesos de auditoría, fusiones, desarrollo tecnológico o prestación de servicios profesionales.

Así pues, todo NDA debe establecer con claridad:

- Qué se considera información confidencial (puede incluir tanto información técnica como comercial).
- Cuál será el plazo de vigencia de la obligación de confidencialidad.
- Qué usos están permitidos y cuáles prohibidos.
- Las excepciones (información de dominio público, información ya conocida por la parte receptora).
- El nivel de seguridad técnica y organizativa exigido para la custodia.
- Consecuencias en caso de incumplimiento (responsabilidad civil, medidas cautelares, cláusulas penales).

Esto los han vuelto herramientas imprescindibles para establecer límites claros frente al uso de tecnologías emergentes que facilitan la duplicación, diseminación o ingeniería inversa de la información compartida[10], especialmente si se toma en cuenta que más allá de la prohibición de divulgar, el NDA impone un deber activo de custodia, es decir, la obligación de proteger la información confidencial contra accesos no autorizados, robos digitales o uso indebido por terceros. Esto se traduce en:

---

[9] Carla De Bona, Protección de la información confidencial en el derecho comparado (Santiago de Chile: Editorial Jurídica de Chile, 2020).

[10] Richard Raysman, *Protecting Trade Secrets and Confidential Information in the Digital Age. The Computer & Internet Lawyer* 39, no. 4.

- Medidas físicas (acceso restringido, archivado seguro).
- Medidas técnicas (encriptación, control de accesos, monitoreo).
- Medidas organizativas (protocolos internos, entrenamiento del personal, uso controlado de software).

Y lo relevante jurídicamente de este deber, es que tiene fundamento constitucional en el derecho a la propiedad privada, intimidad, protección de información, e incluso imagen, y que en entornos empresariales se traduce en una obligación de diligencia reforzada sobre los datos estratégicos y su posible exposición tecnológica[11].

Pero, visto desde la perspectiva práctica, en los últimos años se han hecho común reportajes de empleados y profesionales que usan herramientas como ChatGPT, Google Translate, DeepL, convertidores de PDF a Word online, o transcriptores como Whisper para facilitar sus tareas que, aunque útiles, pueden implicar un riesgo grave de fuga de información cuando se utilizan sin autorización o en versiones abiertas sin cifrado, ni contrato de servicio empresarial.

Los datos ingresados en estos sistemas, incluyendo indicativos, instrucciones, archivos adjuntos o fragmentos de texto, pueden quedar almacenados en servidores de terceros, ser utilizados para entrenar modelos, o incluso ser accesibles a desarrolladores u otros usuarios, lo cual puede constituir una violación del NDA, aunque la intención del usuario no haya sido dolosa. En este sentido, se plantea que los NDAs modernos deben adaptarse a la arquitectura digital del trabajo actual, regulando expresamente el uso de tecnologías de automatización y el procesamiento externo de datos[12]. La solución no es prohibir toda tecnología, sino establecer cláusulas claras sobre:

- Plataformas autorizadas para trabajar con información confidencial.
- Requisitos mínimos de seguridad (versiones empresariales, cifrado de extremo a extremo).
- Prohibición de cargar información sensible en aplicaciones sin contrato ni supervisión.
- Obligación de informar a la otra parte sobre incidentes de seguridad.

Esto cobra mayor importancia cuando se entiende que los NDAs son plenamente exigibles en juicio, incluso aunque no estén acompañados de una relación contractual principal. En muchos sistemas jurídicos, su violación permite solicitar:

---

[11] Carlos Ayala Corao, Derechos fundamentales y nuevas tecnologías (Caracas: Editorial Jurídica Venezolana, 2021)

[12] Roberto Delgado, "El deber de custodia de la información confidencial en tiempos de inteligencia artificial," Revista Iberoamericana de Derecho Digital 8, no. 2

- Medidas cautelares (prohibición de uso, aseguramiento de evidencia).
- Daños y perjuicios, especialmente si se demuestra lucro cesante o daño reputacional.
- Ejecución de cláusulas penales previamente pactadas.

En procesos civiles, comerciales o laborales, los jueces suelen exigir que la información protegida haya sido identificada claramente y que exista una traza razonable de su custodia. Las partes deben probar que actuaron con diligencia en evitar su exposición, lo que ha llevado que organismos como la WIPO (Organización Mundial de la Propiedad Intelectual) han propuesto cláusulas modelo adaptadas al entorno digital. Una de ellas reza:

> "La Parte Receptora se compromete a no introducir Información Confidencial en herramientas de inteligencia artificial, plataformas de traducción automática, sistemas de conversión digital o cualquier otro entorno computacional externo sin autorización escrita expresa de la Parte Reveladora"[13].

## *3. Información confidencial, pilar del ejercicio comercial global*

Es todo dato, conocimiento, documento, procedimiento o fórmula que posee valor económico o estratégico para una persona natural o jurídica, y que no es de dominio público cuya protección no depende exclusivamente del registro legal, como ocurre con las patentes o marcas, sino de su carácter reservado y del esfuerzo que su titular haya hecho para mantenerla oculta.

La definición de la WIPO establece que la información confidencial comprende conocimientos técnicos o comerciales no divulgados que una empresa protege porque le otorgan una ventaja competitiva[14] y puede abarcar desde fórmulas químicas, códigos fuente, manuales internos y listas de clientes, hasta estrategias de marketing o datos financieros.

Desde el punto de vista jurídico, la información confidencial se caracteriza por ser un activo intangible de naturaleza híbrida pues, por un lado, es un bien económico susceptible de protección y valoración (por ejemplo, en balances contables o contratos de cesión) y, por otro, es objeto de relaciones jurídicas, ya que genera derechos de exclusividad y deberes de custodia, aun sin necesidad de inscripción o formalidad alguna.

---

[13] WIPO, *Confidentiality Clauses in IP Agreements: Model Provisions and Guidance* (Ginebra: WIPO, 2021)

[14] WIPO, Trade Secrets and Confidential Information: A Guide for Businesses (Ginebra: WIPO, 2018)

Constituye una figura sui generis, que se ubica entre los secretos empresariales y los bienes jurídicos protegidos por la buena fe contractual[15], lo que explica que su protección se sustente en diversas fuentes: la ley, los contratos (NDAs), la doctrina del enriquecimiento sin causa y la responsabilidad extracontractual, generando responsabilidad civil, e incluso penal, cuando existe uso indebido, apropiación fraudulenta, competencia desleal o violación deliberada del deber de confidencialidad.

Así, para que un dato pueda ser calificado como "confidencial", deben cumplirse al menos tres condiciones, ampliamente reconocidas por la jurisprudencia y doctrina internacional:

- Valor económico: debe ser útil o estratégico para la parte que lo posee.
- Carácter reservado: no debe ser fácilmente accesible al público o a competidores.
- Medidas de protección: la parte titular debe haber adoptado medidas razonables para mantener su confidencialidad.

De esta manera lo ratificó el Tribunal de Casación de Francia en el fallo Société B. c/ Société C., señalando que "no puede invocarse el carácter confidencial de una información si la empresa no demuestra haber tomado medidas activas para su resguardo[16]. Por lo que el uso cotidiano de herramientas de IA generativa, plataformas de traducción automática, sistemas de almacenamiento en la nube, y conversores digitales gratuitos, ha multiplicado los riesgos de fuga o exposición no intencional de información sensible. Por ejemplo:

1. Cargar un contrato confidencial en un traductor automático gratuito puede implicar su procesamiento por servidores externos.
2. Enviar bases de datos a plataformas de conversión puede dejar trazas accesibles.
3. Ingresar *prompts* con datos sensibles en herramientas como ChatGPT o Copilot puede hacer que esa información sea almacenada temporalmente o utilizada para entrenamiento futuro.

En ese contexto, la confidencialidad no puede depender de la tecnología, sino de una arquitectura jurídica de protección, integrada por cláusulas contractuales, códigos de conducta y protocolos internos[17].

---

[15] Isabel Rodríguez Martínez, La protección de la información confidencial en el derecho privado (Madrid: Marcial Pons, 2017),

[16] Cour de cassation [Francia], 3e chambre civile, 6 juillet 2021, no. 19-25061

[17] Yoshiko Nakanishi, "Confidential Information and Data Leakage in AI Tools: Legal Implications in Japan," Kyoto Journal of Law and Technology 22, no. 1

### *3.1. Ampliar el concepto de "información confidencial"*

Para cubrir estos riesgos, se recomienda ampliar el alcance de las cláusulas de confidencialidad pues no basta con referirse genéricamente a documentos, datos técnicos o estrategias de negocio; hoy la noción debe incluir expresamente *prompts* o consultas introducidas en herramientas de IA, así como *outputs* generados por IA que reproduzcan datos[18]. De esta forma, cualquier dato ingresado a un sistema de IA queda protegido por el NDA, redefiniendo qué se considera confidencial, para que el NDA cubra nuevas formas de manejo de la información (IA, traducción, conversión).

Este enfoque también aplica a los códigos de ética pues muchas organizaciones deben aclarar en su reglamento interno que la información digital, incluyendo la inserción en sistemas de IA o el envío a servicios de traducción en línea, requiere el mismo grado de secreto que un documento impreso.

Una medida común es prohibir explícitamente el uso no autorizado de IA pública u otras herramientas en el tratamiento de información confidencial, incluyendo cláusulas que establecen cosas como: "Queda expresamente prohibido introducir información confidencial en sistemas de inteligencia artificial generativa, salvo consentimiento expreso y por escrito de la parte titular". Incluso, en numerosos contratos ya se está incluyendo un veto al uso de IA pública sin autorización previa, utilizando un lenguaje específico que refiere: prohibición de cargar, procesar o divulgar información sensible en modelos de IA accesibles públicamente[19]

Sin embargo, esta prohibición implica una negación total a la tecnología, y no un control riguroso del contexto de uso; se puede flexibilizar la restricción contemplando "seguridad razonable" o herramientas certificadas. Por ejemplo, si una empresa quiere permitir IA en ciertos casos, el contrato puede exigir medidas de seguridad: sólo usar versiones empresariales con garantías contractuales (como Copilot for Business), requerir servidores privados o locales, o uso de software de código abierto ejecutado internamente. De este modo, queda prohibido el uso indiscriminado de plataformas

---

[18] Stacey Heller "*Since AI systems rely on large datasets for training, there is an increased risk that confidential information could be fed into AI models during this stage. AI systems also have a capacity for "memorization." Unlike people who forget information over time, AI models can perpetually retain confidential information embedded in their system". Confidentiality Provisions, Blog.* Disponible en https://www.outsidegc.com/blog/incorporating-ai-training-language-in-confidentiality-provisions#:~:text=,%E2%80%9D

[19] Mathias Avocats (2024) *L'intelligence artificielle dans les contrats : enjeux et bonnes pratiques Il est essentiel de définir précisément les obligations des parties, notamment les stipulations doivent permettre de garantir l'exactitude et la qualité des résultats fournis par l'IA, encadrer l'utilisation des données et prévoir les modalités de gestion des droits de propriété intellectuelle sur les résultats obtenus et ce, sans oublier les garanties concernant les données utilisées pour générer les résultats.* Disponible en: *https://www.avocats-mathias.com/conformite/lintelligence-artificielle-dans-les-contrats-enjeux-et-bonnes-pratiques#:~:text=Il%20est%20essentiel%20de%20d%C3%A9finir,utilis%C3%A9es%20pour%20g%C3%A9n%C3%A9rer%20les%20r%C3%A9sultats*

externas, pero se habilita el uso de IA bajo entornos controlados, equilibrando la innovación y eficiencia con la protección de datos.[20]

Las cláusulas pueden exigir pruebas de seguridad por parte del proveedor de IA, por ejemplo, debe demostrar que no retiene ni reutiliza los datos ingresados, incluso pudiendo solicitar documentación técnica donde se garantice que la herramienta no almacena la información, cifra los inputs y separa lógicamente los datos de cada cliente.

## *4. Responsabilidades frente a terceros y proveedores externos*

La regulación debe extenderse a subcontratistas y terceros, haciendo que cualquier persona o entidad que acceda a la información confidencial deberá respetar las mismas restricciones (incluyendo la prohibición de subir datos a IA pública), de lo contrario, un tercero podría quebrantar las reglas internas (por ejemplo, un traductor *freelancer* que usa una IA online) sin consecuencias.

Además, al negociar con proveedores de servicios lingüísticos o tecnológicos, conviene incluir cláusulas modelo específicas para IA, donde se propone elaborar adendas estándar para IA, donde se aborden no solo la confidencialidad sino también la precisión, el uso de herramientas de código abierto, y la titularidad de contenidos generados haciendo que se considere explícitamente el uso de soluciones de terceros (ya sea un proveedor de IA comercial o software libre) en el acuerdo.

## *5. Integración con la ingeniería inversa*

La ingeniería inversa consiste en analizar un producto, sistema o software para descubrir sus componentes, funcionamiento interno o principios de diseño. Aunque originalmente asociada al ámbito industrial y electrónico, hoy se aplica ampliamente a software, bases de datos, modelos de inteligencia artificial, y algoritmos cuya finalidad puede ser técnica (interoperabilidad, depuración, aprendizaje) o competitiva (imitación, mejora, explotación).

La ingeniería inversa es un proceso legítimo en muchos casos, y esencial en ecosistemas tecnológicos abiertos. Sin embargo, también puede rozar los límites de la legalidad cuando se aplica sobre sistemas protegidos por derechos de propiedad intelectual o confidencialidad[21]. No está prohibida por defecto en la mayoría de los sistemas jurídicos, pero su legalidad depende de factores clave:

---

[20] Simon Hodgkins, Confidentiality in the Age of AI: Why Your NDAs Probably Require an Upgrade. Disponible en: https://simonhodgkins.medium.com/confidentiality-in-the-age-of-ai-28d0d2a1e602

[21] Andrés Rueda, Derecho informático y contratos tecnológicos, 5.ª ed. (Bogotá: Temis, 2021)

- Si el objeto está protegido por secreto comercial, copyright o patente.
- Si existen cláusulas contractuales que la limitan expresamente.
- Si su uso persigue fines legítimos o infringe derechos de terceros.

En el derecho de la Unión Europea, la Directiva 2009/24/CE[22] sobre programas de ordenador permite la ingeniería inversa con fines de interoperabilidad, siempre que no se use para desarrollar un producto similar, lo que ha sido reafirmado por el TJUE en casos como *SAS Institute Inc. v. World Programming Ltd*[23]. En Estados Unidos, la doctrina del *fair use* permite ciertos usos legítimos, como el análisis técnico o educativo, pero la jurisprudencia ha sancionado su uso con fines comerciales desleales.

En América Latina, el tratamiento ha sido más restrictivo, aunque algunos países como Brasil permiten la ingeniería inversa en ciertos supuestos relacionados con competencia leal y acceso a la tecnología.[24]

Pero, ¿cuándo no está dentro de los parámetros legales? Cuando:

- Se realiza en contra de lo que establece un contrato (por ejemplo, una cláusula de un NDA que la prohíba).
- Supone eludir medidas técnicas de protección, como cifrado o restricciones de acceso.
- Busca copiar sustancialmente un software protegido por derechos de autor.
- Se utiliza para acceder a información confidencial sin consentimiento.

La ingeniería inversa no es una infracción per se, pero puede convertirse en un acto de competencia desleal o violación de secreto comercial cuando afecta derechos legítimos del desarrollador original[25], por lo que en entornos comerciales, muchas licencias de software y contratos de confidencialidad prohíben expresamente la ingeniería inversa. Este tipo de cláusula se considera válida y exigible en la mayoría de las jurisdicciones, siempre que esté claramente redactada; por ejemplo:

---

[22] La Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, es la norma de la Unión Europea que regula la protección jurídica de los programas de ordenador (software). Es la ley europea que establece cómo se protege legalmente el software como obra intelectual y qué puede o no puede hacer un usuario con un programa.

[23] En SAS Institute Inc. v. World Programming Ltd (C-406/10, TJUE, Tribunal de Justicia de la Unión Europea, 2012), el TJUE determinó que, conforme a la Directiva 2009/24/CE, la funcionalidad de un programa, su lenguaje de programación y los formatos de archivos de datos no están protegidos por derechos de autor, por no constituir una forma de expresión del software. Asimismo, el TJUE sostuvo que un usuario legítimo puede observar, estudiar o probar el funcionamiento del programa para reproducir su comportamiento, siempre que no se copie el código fuente ni el código objeto.

[24] Danilo Doneda, *"Segredos comerciais e engenharia reversa: uma aproximação jurídica," Revista de Direito da Concorrência* 18, no. 1 (2020): 89–106.

[25] Serge Gervasoni, *Droit de l'informatique et de l'Internet, 8.ª ed.* (Paris: Dalloz, 2022), 201–202.

> "La Parte Receptora se compromete a no efectuar ingeniería inversa, descompilación o desensamblaje de ningún software, modelo, base de datos o sistema facilitado por la Parte Reveladora, salvo autorización expresa por escrito"[26].

No obstante, en entornos regulatorios o públicos (por ejemplo, contratación estatal o software educativo), estas restricciones pueden ser revisadas para asegurar el interés público, la transparencia o la interoperabilidad, pues prohibir la ingeniería inversa de forma absoluta puede perjudicar la innovación, la transparencia y la seguridad digital. Por ejemplo, algunos especialistas en ciberseguridad utilizan ingeniería inversa para detectar vulnerabilidades, y los desarrolladores de software libre la emplean para crear herramientas compatibles.

En este sentido, se ha propuesto una regulación diferenciada que permita ciertos usos "justos" o socialmente beneficiosos, especialmente en inteligencia artificial, lo que implica:

- Distinguir entre ingeniería inversa legítima y copia maliciosa.
- Establecer criterios claros en los contratos (con finalidades permitidas o excepciones).
- Articular la cláusula con los derechos de propiedad intelectual, el interés público y la ciberseguridad.
- Evaluar su impacto sobre la información confidencial o protegida.

En síntesis, el objetivo no debe ser prohibir indiscriminadamente, sino establecer límites contractuales claros que orienten el uso responsable de esta técnica, protejan los activos de la empresa y permitan innovación compatible con la legalidad, por ejemplo, se puede autorizar la inspección funcional mínima (para comprobar compatibilidad), pero prohibir la reproducción de secretos con fines propios.

En todo caso, la ingeniería inversa está ligada a la confidencialidad: forzar un NDA que prohíba todo análisis podría ser percibido como intransigente. En la regulación inteligente, se busca equilibrar la protección del know-how con la flexibilidad técnica, donde una empresa podría exigir, por ejemplo, que cualquier descubrimiento técnico relevante sea notificado y se regule su uso (en lugar de simplemente castigar la violación).

---

[26] WIPO, *Model Provisions on Trade Secret Protection* (Ginebra: WIPO, 2021), cláusula 8.4.

## *6. Principios de "regulación inteligente" frente a la prohibición absoluta*

Estas cláusulas no deben entenderse o aplicarse como vetos puros, sino como una normativa inteligente que facilite el buen uso de tecnologías; en lugar de prohibir todo recurso tecnológico, se propone permitir el uso seguro y responsable con pautas claras. Por ejemplo, pueden autorizarse herramientas de IA siempre que sean entornos corporativos, o que cuenten con garantías de privacidad, lo que significa que, bajo condiciones contractualmente definidas, los empleados sí pueden apoyarse en la IA para mejorar procesos, pero sin exponer datos sensibles.

La regulación inteligente implica fomentar la alfabetización tecnológica, no el aislamiento del mundo que ya está aquí y no va a retroceder; la alfabetización digital no puede ser opcional y los profesionales deben adquirir competencias tanto técnicas como éticas en IA, para que su utilización sea responsable y rigurosa[27], haciendo hincapié en operar en entornos seguros. Para ello, desde el punto de vista del *compliance*, se deben crear políticas internas claras que establezcan qué datos pueden usarse con IA y cuáles están prohibidos.

Este marco regulatorio inteligente tiene beneficios claros: permite a los trabajadores aprovechar herramientas modernas (traducción automática, asistentes de redacción, análisis de datos) para hacer negocios más ágiles y eficaces, sin temer violar la confidencialidad y al mismo tiempo, refuerza la seguridad jurídica, siempre que las reglas estén establecidas.

## *7. Herramientas de traducción, conversión y software libre*

En un contexto globalizado, el personal suele necesitar traducir documentos técnicos o legales y convertir archivos entre formatos (por ejemplo, de PDF a Word) como parte de su trabajo cotidiano y las herramientas de IA basadas en la nube, hacen que estas tareas sean muy rápidas, pero conllevan riesgos de seguridad.

Un informe de Polilingua explica que la mayoría de herramientas de traducción por IA envía el contenido a servidores remotos, donde puede almacenarse indefinidamente y utilizarse para entrenar modelos y, en la práctica, esto significa que un texto confidencial enviado para traducir podría terminar formando parte de una base de datos pública[28].

---

[27] Laura Basch (2025) Inteligencia artificial generativa y ética profesional. Especialistas en la intersección de derecho y tecnología enfatizan la necesidad de prudencia. Isabel Rodríguez, directora de Servicios Profesionales en Accenture España, advierte que si bien la IA ofrece gran potencial en servicios jurídicos, su uso debe ser "responsable y riguroso" para evitar sesgos y discriminación. Señala los riesgos de emplear IA de fuente abierta (como ChatGPT) en tareas legales: problemas de fiabilidad de la información, falta de contexto jurídico local y vulneraciones de privacidad y confidencialidad.

[28] Otilia Munteanu, Polilingua (2025) Privacidad y seguridad de los datos en la IA y traducción: Lo que debes saber. Con la

Para mitigar esto, el artículo de Polilingua sugiere estrategias prácticas: usar servicios conformes con la normativa (por ejemplo, soluciones compatibles con GDPR para datos sensibles) y, de ser posible, preferir software de código abierto o versiones locales que no envíen los datos a servidores externos. En este sentido, es importante que el NDA o código de ética indique qué herramientas de traducción o conversión están permitidas.

Permitir explícitamente el uso de plataformas de software libre que garanticen retención mínima de datos, como OmegaT es un escenario ideal, pero, al contrario, los servicios comerciales gratuitos (Google Translate o DeepL sin licencia empresarial) suelen procesar el texto en la nube pública y deberían estar vetados para información confidencial. En cuanto a conversión de archivos se siguen principios semejantes pues, si un empleado convierte un PDF confidencial en Word usando una herramienta online pública, podría cargar datos sensibles en el servidor de esa página.

En síntesis, debe quedar explícito en el código de conducta y en los contratos, qué herramientas digitales de traducción o conversión se permiten y en qué condiciones. Esto evita ambigüedades y enseña al personal a apoyarse en buenas prácticas tecnológicas. Por ejemplo, un código de ética prudente incluirá recomendaciones como: "Solo usar herramientas de traducción certificadas y desactivar la opción de aprendizaje automático cuando sea posible", o "no subir documentos internos a servicios gratuitos de conversión online"[29]. Por supuesto, se recomienda no establecer proveedores directamente, (i) porque las circunstancias de la herramienta pueden cambiar, y (ii) para evitar afiliaciones innecesarias; puede especificarse el tipo de herramientas y sus características técnicas, y derivar a que los colaboradores hagan consultas al equipo técnico.

## *8. Negocios exitosos y relaciones seguras mediante regulación inteligente*

La adopción de un enfoque regulador inteligente tiene múltiples ventajas para la empresa. En primer lugar, protege los activos intangibles (propiedad intelectual, know-how, datos de clientes) al tiempo que deja la puerta abierta a la innovación. Actualizar los NDA se convierte en una señal de confianza para los terceros: demuestra que entiende la tecnología y que gestiona activamente los riesgos asociados pues, de no hacerlo, estos son algunos de los problemas típicos sin cláusulas específicas

adopción generalizada de las herramientas de traducción basadas en inteligencia artificial (IA) en entornos profesionales, su comodidad y rapidez a menudo eclipsan una preocupación crítica: la privacidad de los datos.

[29] Otilia Munteanu, Polilingua (2025) Privacidad y seguridad de los datos en la IA y traducción: Lo que debes saber.

1. **Filtración involuntaria (constructive disclosure):** subir archivos a traductores/convertidores con condiciones opacas (p.ej., autorizar "mejora del servicio" o conservar muestras) puede quebrar la cláusula de confidencialidad y las políticas de retención.[30]
2. **Trazabilidad y auditoría nula:** sin logs y controles de acceso (quién, qué, cuándo, con qué herramienta), es imposible demostrar cumplimiento o contener incidentes[31].
3. **Ingeniería inversa por terceros/algoritmos:** cadenas de prompts, metadatos y outputs podrían permitir deducir procesos internos o parámetros estratégicos de un modelo/negocio; los NDAs deben cerrar esa puerta.[32]
4. **Desalineación multi-jurisdiccional:** proveedores globales de IA operan bajo marcos distintos (UK, UE, Japón, EE. UU.), lo que exige cláusulas puente para confidencialidad y datos.[33]

En sectores altamente regulados o intensivos en manejo de datos, como la banca, el marketing o la asesoría jurídica, los clientes exigen garantías no solo tecnológicas, sino contractuales y éticas frente al uso de herramientas de inteligencia artificial. Una organización que establece políticas claras y transparentes sobre el uso autorizado de IA transmite madurez digital, previsión jurídica y compromiso con la confidencialidad, lo que no solo mitiga riesgos de filtración, sino que consolida la confianza y estabilidad en las relaciones comerciales, favoreciendo la firma de contratos más duraderos y sólidos.

La regulación inteligente, aquella que combina apertura tecnológica con límites razonables, también tiene impacto en la eficiencia interna pues, permitir el uso de IA generativa, sistemas de traducción automatizada o plataformas de asistencia textual puede agilizar tareas repetitivas, siempre que se impongan protocolos claros: revisión humana obligatoria, restricción de datos sensibles, y trazabilidad de los documentos procesados. Este enfoque evita el riesgo de delegar decisiones sin control pues la delegación a la IA, no exime de la obligación de verificar, controlar y evaluar cada

---

30 Guidance on AI and data protection (2023). Disponible en: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/?utm_source=chatgpt.com

31 *National Institute of Standards and Techonology. U.S Department of Commerce (2023) Artificial Intelligence Risk Management Framework* (AI RMF 1.0)

32 *U.S Government (2016). Defend trade secrets act of 2016*

33 *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)*

resultado[34], reafirmando que la tecnología no reemplaza la ética profesional: la refuerza si se aplica con conciencia y conocimiento.

Además, la regulación inteligente contribuye a evitar prácticas que comprometan la integridad documental, como ha quedado evidenciado en dos recientes pronunciamientos judiciales en Argentina en el caso M.J.L. c/ Peugeot Citroen Argentina S.A y otra, donde la Cámara de Apelaciones en lo Civil, Comercial, Familia y Minería de General Roca detectó la inclusión de citas jurisprudenciales inexistentes en los escritos de ambas partes, presumiblemente generadas con IA. Aunque no se aplicaron sanciones, el tribunal enfatizó que ni siquiera la buena fe exime del deber profesional de verificar la existencia y exactitud de las fuentes citadas[35].

Un caso análogo se dio en el expediente Acevedo Gerardo Gabriel c/ Cáceres Mareco y Agrosalta, tramitado ante la Cámara de Morón, donde el recurso fue declarado desierto por basarse en jurisprudencia ficticia, como un supuesto fallo "Barrios" que no figuraba en registros oficiales. La sala asoció esta práctica al fenómeno de las "alucinaciones" de la inteligencia artificial generativa, donde se crean resultados verosímiles pero falsos; aunque no hubo sanción, se instó a los abogados a ejercer un uso responsable de estas herramientas y se notificó al Colegio de Abogados local para promover capacitaciones sobre buenas prácticas tecnológicas[36].

Estas decisiones judiciales revelan una paradoja: el uso indiscriminado o sin control de IA no solo puede afectar la validez de un documento legal, sino erosionar la credibilidad profesional, lo que representa un riesgo reputacional para firmas, empresas y sectores enteros. En cambio, la incorporación transparente de cláusulas sobre IA en los códigos de ética y NDAs demuestra una voluntad de actuar con integridad, pues lejos de inhibir el uso de tecnología, este enfoque empodera a los trabajadores, clarifica los límites y crea condiciones contractuales claras.

## CONCLUSIONES

La regulación inteligente crea un círculo virtuoso: claridad contractual + ética aplicada = confianza = flujo seguro de información = mayor velocidad de negocio. En un entorno donde las autoridades publican guías para conciliar innovación y derechos, y marcos regulatorios claros proveen estándares de referencia, las empresas que anticipan

[34] Laura Basch (2025) Inteligencia artificial generativa y ética profesional.

[35] Diego Fernández et al., "Citas falsas generadas con IA y el deber de verificación: dos fallos argentinos advierten riesgos," Marval O'Farrell Mairal, octubre 2025.

[36] Cámara de Apelación en lo Civil y Comercial de Morón, fallo "Acevedo Gerardo Gabriel c/ Caceres Mareco y Agrosalta", 2025.

cláusulas sobre IA, traducción y conversión reducen litigios y aumentan su atractivo como contrapartes confiables. Desde la perspectiva venezolana y latinoamericana, la adopción de buenas prácticas internacionales es crucial para la inserción competitiva y la cooperación transfronteriza. La doctrina local (Vaudo Godina) y los estudios regionales sugieren fortalecer la educación y la cultura corporativa para que las cláusulas no sean un obstáculo, sino un andamiaje habilitante.

Para finalizar, se proponen modelos de cláusulas que pueden ser utilizadas como primeros pasos tanto en contratos como en políticas, manuales o códigos de la compañía; su uso debe venir acompañado de la adecuación al contexto de cada persona o empresa que desee usarlo.

- Uso ético de herramientas digitales: "El personal podrá utilizar herramientas de inteligencia artificial, traducción automática o conversión de archivos únicamente en plataformas autorizadas por la organización y bajo los principios de minimización, trazabilidad y responsabilidad. Queda prohibido introducir Información Confidencial o datos personales en servicios no aprobados. Todo contenido generado por inteligencia artificial deberá ser revisado y validado por una persona responsable antes de su uso o difusión. El incumplimiento de estas obligaciones será considerado infracción grave al Código de Ética."

- Uso de herramientas tecnológicas de transformación de información: "La Parte Receptora se compromete a no introducir, cargar ni procesar Información Confidencial mediante herramientas de inteligencia artificial, traductores automáticos o convertidores de archivos de terceros sin autorización previa y por escrito de la Parte Reveladora. Cualquier uso autorizado deberá limitarse a entornos empresariales que ofrezcan exclusión de entrenamiento, control de retención y registros de auditoría. La Parte Receptora adoptará medidas razonables para impedir el acceso o uso no autorizado de la Información Confidencial, y cualquier divulgación resultante de tales actos constituirá incumplimiento material de este acuerdo."

- Ingeniería inversa: "La Parte Receptora no realizará, ni permitirá que terceros realicen, ingeniería inversa, descompilación, desensamblaje, análisis estructural, análisis algorítmico ni ningún otro procedimiento técnico sobre la Información Confidencial o cualquiera de sus derivados, incluyendo resultados generados con herramientas de inteligencia artificial que incorporen datos, estrategias, algoritmos, procesos o know-how de la Parte Reveladora. En caso de que la Parte Receptora, de manera involuntaria o incidental, obtenga conocimiento técnico, funcional o comercial susceptible de ser considerado valioso, reproducible o sensible mediante técnicas similares, se obliga a:

a. Notificar inmediatamente a la Parte Reveladora;
b. Abstenerse de usar o compartir dicho conocimiento sin autorización previa por escrito;
c. Entregar un resumen técnico o informe detallado de los hallazgos si así lo solicita la Parte Reveladora, y
d. Destruir cualquier copia no autorizada o derivado técnico si lo requiere la Parte Reveladora.

Esta obligación subsistirá incluso tras la terminación del contrato y se considerará parte del deber de custodia y protección reforzada de la información confidencial.

## BIBLIOGRAFÍA

Armas, David A. 2024. "Un enfoque de la inteligencia artificial para la protección de datos personales." Revista Tecnológica-Educativa Docentes 2.0.

Auris Legal. 2024. "La IA no exime la verificación profesional: implicaciones éticas y jurídicas.

Bertoni, Eduardo A., comp. 2012. Hacia una Internet libre de censura: propuestas para América Latina. Buenos Aires: Universidad de Palermo.

BID (Cabrol, Marcelo; Natalia González A.; Cristina Pombo; Roberto Sánchez). 2022. "Adopción ética y responsable de la IA en ALC." En La Inteligencia Artificial y la Protección de Datos… (comp. ITEI)

Carpinelli, Lucía, Diego Fernández, Gustavo P. Giay, Manuela Adrogué, Josefina Barbero, Sofía Negri y Mariano Zanotti. 2025. "LegalTech y el uso responsable de la inteligencia artificial." Marval O'Farrell Mairal, octubre 2025.

CNIL (Commission Nationale de l'Informatique et des Libertés). 2023. "IA y protección de datos: recomendaciones regulatorias."

Congreso de EE. UU. 2016. *Defend Trade Secrets Act of 2016* (DTSA), Pub. L. 114-153 (texto oficial y 18 U.S.C. § 1836).

Congress.gov. 2016. *Defend Trade Secrets Act of 2016.*

Duke Law (Center for the Study of the Public Domain). s. f. *Trade Secrecy & Preemption.* Capítulo (PDF) vías lícitas: ingeniería inversa/descubrimiento independiente

Hodgkins Simon. 2023. *AI Tools and the Danger of Confidentiality Breach*. Medium.

Information Commissioner's Office (ICO). 2023. *AI and Data Protection Risk Toolkit.*

INPLP. 2023. *Generative AI and the Protection of Personal Information under Japanese Law.* Alerta PPC sobre ingresar datos personales en IA.

IPWatchdog. 2021. *Reverse Engineering and the Law: Understand Restrictions and Minimize Risks*. (síntesis jurisprudencial: *Kewanee Oil*; *Bonito Boats*)

METI/PPC (*Ministry of Economy, Trade and Industry, Personal Information Protection Commission*). 2024. *AI Governance Guidelines and Compliance Models in Japan.* Japón. https://meti.go.jp

Morimoto, Hiroshi, y Akiyama, Keiko. 2023. *AI Ethics in Japanese Corporations: A Governance Model for Generative Tools. Journal of Asia Business Compliance.*

NIST. 2023. *AI Risk Management Framework. National Institute of Standards and Technology.*

Ocando Ibarra, Thomas A., y Marieugenia Mas y Rubí. 2023. La identidad digital soberana para la protección de datos personales en Venezuela. Cuestiones Jurídicas. https://doi.org/10.5281/zenodo.16368306.

Outside GC. 2023. *What Companies Should Know About ChatGPT and Trade Secrets.*

Polilingua. 2024. *Translation and Confidentiality in the Age of AI.*

Proyecto GUIA (comp.). 2020. Inteligencia Artificial en América Latina y el Caribe. Ética, gobernanza y políticas públicas.

Red por los Derechos Digitales (comp.). 2021. La protección de datos personales en Venezuela. Ensayo (PDF).

Sprintlaw UK. 2023. *Can You Upload Confidential Info into ChatGPT?*

Tribunal de Casación de Francia. 2020. *Société B. c/ Société C.* (Jurisprudencia sobre confidencialidad y deber de protección).

Tribunal de General Roca. 2025. M.J.L. c/ Peugeot Citroën Argentina S.A. y otra s/sumarísimo.

Tribunal de Morón. 2025. Acevedo Gerardo Gabriel c/ Cáceres Mareco y Agrosalta Cooperativa.

Vaudo Godina, José Alejandro. 2022. La confidencialidad y los datos en la era digital: reflexiones desde el derecho venezolano. Revista Venezolana de Derecho Comercial.

WIPO (World Intellectual Property Organization). 2022. *Trade Secrets: Model Clauses and Best Practices.*