

# HOLA ALEXA, ¿ME AYUDAS CONTRA LA EVASIÓN FISCAL?



¿Es útil? (0) (0)

Florencia Ungra  26/06/2025

## SUMARIO:

La autora analiza las herramientas que la Inteligencia Artificial (IA) ofrece para combatir el fraude y la evasión fiscal, fortalecer el cumplimiento voluntario de obligaciones tributarias y optimizar la recaudación del Fisco. Explora el panorama en el derecho comparado y las propuestas para su implementación en Argentina. Plantea el desafío que implica equilibrar el uso de IA en la fiscalización, con el respeto a los principios de legalidad, privacidad y protección de datos personales, evitando que los ciudadanos sean tratados indiscriminadamente como evasores.

Esta doctrina fue publicada en:

- Temas de Derecho Penal y Procesal Penal

## LA IMPLEMENTACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA LUCHA CONTRA LA EVASIÓN FISCAL

*“Mi barómetro para conocer las garantías de tranquilidad que ofrece un país las busco en el estado de su hacienda pública y, al mismo tiempo, en las bases de su gobierno.”<sup>[1]</sup>*  
General José de San Martín

*“El futuro de la humanidad depende de cómo usemos la Inteligencia Artificial.”<sup>[2]</sup>*  
Papa Francisco

## I - INTRODUCCIÓN

La percepción de impuestos se remonta al origen de todos los Estados en general y, en particular, al nuestro. Desde 1853, la [Constitución Nacional](#) ha considerado esta potestad como un pilar fundamental para la subsistencia y el financiamiento del Estado.<sup>[3]</sup>

Fue Wagner uno de los primeros teóricos que concibió al impuesto no como un elemento dañino o “mal menor”, sino como un útil instrumento de modificación de la distribución de la renta nacional en sentido igualitario<sup>[4]</sup> y de política fiscal puesta al servicio de la economía.<sup>[5]</sup>

Aunque el mundo ha cambiado drásticamente desde entonces, la naturaleza de los tributos sigue siendo la misma, al igual que el desafío de optimizar la recaudación fiscal. En este sentido, el ámbito tributario no puede ni debe desaprovechar los avances tecnológicos, especialmente en la lucha contra el fraude fiscal.

En este contexto, todo apunta a que las herramientas que ofrece la Inteligencia Artificial (IA) desempeñarán un papel crucial en el futuro de la Administración Tributaria (AT), ayudando al Fisco a fortalecer el cumplimiento voluntario, incrementar la recaudación e identificar la tipología de actuación de los evasores.

A continuación, analizaremos las herramientas que la IA ofrece y el panorama en el derecho comparado, explorando propuestas para su implementación en Argentina.

Una estrategia integral para que la Administración Tributaria minimice las prácticas de elusión y evasión fiscal debe incluir un elemento clave: la obtención de pruebas que acrediten las malas prácticas de los contribuyentes evasores sin afectar los derechos de quienes cumplen con sus obligaciones. Es fundamental evitar generalizaciones que traten a todos como evasores, ya que ello vulneraría los derechos de los ciudadanos que contribuyen de manera responsable al sistema tributario.

## II - LA INVESTIGACIÓN DE DELITOS FISCALES CON HERRAMIENTAS DE IA

La lucha contra la evasión fiscal llevó al legislador a recurrir al Derecho Penal como herramienta para garantizar la protección del bien jurídico tutelado mediante la aplicación de sanciones penales.

Los delitos contra la Hacienda Pública constituyen el punto de convergencia de dos ramas del ordenamiento jurídico: el Derecho Tributario y el Derecho Penal. El primero aporta todo su sistema de garantías y límites, indispensable dada la gravedad que comporta la pena, manifestación de la violencia legítima del Estado. El segundo brinda todos los elementos necesarios para delimitar el hecho punible.<sup>[6]</sup>

Hasta la promulgación de la [ley 23771](#) en febrero de 1990, las conductas vinculadas a la defraudación fiscal eran sancionadas dentro de un régimen contravencional establecido por la [ley 11683](#) de

procedimiento fiscal.

No obstante, quedó en evidencia la necesidad de considerar estas acciones defraudatorias no como meras infracciones tributarias, sino como verdaderos delitos, es decir, conductas reprochables que merecen penas.

Así, la [ley 23771](#) definió una política criminal tributaria significativa, tipificando diversas conductas dirigidas a atentar contra la estabilidad financiera del Estado.<sup>[7]</sup>

Sin embargo, la normativa vigente no ha logrado cumplir completamente con las expectativas en cuanto a su eficacia para desalentar la evasión fiscal. Una de sus principales falencias radica en la falta de celeridad en la investigación de los delitos tributarios, ámbito en el que la IA puede ofrecer respuestas innovadoras y soluciones eficientes.

Dentro de la informática, las tecnologías de IA son un campo vinculado a la computación cognitiva que tiene como objetivo desarrollar máquinas y sistemas capaces de realizar tareas basadas en algoritmos que emulan a las labores que se consideran propias de las funciones humanas sapientes y cognoscitivas, como el razonamiento o el aprendizaje. Dichos algoritmos se componen de códigos informáticos y operaciones lógicas que contienen instrucciones para el análisis rápido de una cantidad masiva de datos en bruto y su transformación para convertirlos en información con valor agregado.<sup>[8]</sup>

La Organización Mundial de la Propiedad Intelectual (OMPI) define a la IA como un campo dentro de la informática que tiene como objetivo desarrollar sistemas capaces de realizar tareas como percepción, interacción con el lenguaje o resolución de problemas basada en algoritmos, que se traducen en códigos informáticos que contienen instrucciones para el análisis rápido y la transformación de datos en conclusiones, información u otros resultados (Organización Mundial de la Propiedad Intelectual, 2024). La caracterización de un sistema como la IA debe basarse en la existencia y utilización conjunta de cinco capacidades: descubrir, predecir, justificar, actuar y aprender.<sup>[9]</sup>

Cuatrecasas Monforte<sup>[10]</sup> dividió las herramientas de IA de utilidad al Derecho Penal:

- a) de predicción y evaluación de riesgos;
- b) de investigación de delitos, y
- c) de tramitación.

Y es que, si bien los algoritmos no pueden predecir el futuro, sí pueden estimar la probabilidad de que algo suceda basándose en los datos ya existentes. Estas herramientas computacionales inteligentes tienden a aumentar la productividad de los organismos de inspección tanto en la recuperación de ingresos como en la acción preventiva, anticipándose a las acciones de evasión fiscal.<sup>[11]</sup>

### III - LOS DATOS Y LA *MACHINE LEARNING*: PRIMERA APROXIMACIÓN

#### a) Los datos

¿Por dónde empezar? Por los datos<sup>[12]</sup>. El derecho es, entre otras cosas, un conjunto de datos susceptibles de ser analizados y procesados por una máquina<sup>[13]</sup>. Los datos son los lentes por los que conocen el mundo los algoritmos de modelos de aprendizaje automático (AA). La mala calidad de los datos -ya sea por sesgos<sup>[14]</sup> o por falta de alineación con el problema a resolver- impacta directamente en la precisión de las predicciones. Además, la recopilación y conservación de datos irrelevantes no solo supone un desperdicio de recursos, sino que también aumenta innecesariamente los riesgos legales y de seguridad, dificultando la identificación y el aprovechamiento de información clave. Entonces, ¿cómo podemos garantizar que los datos recopilados sean pertinentes y cumplan con los requisitos regulatorios?

Los datos deben ser<sup>[15]</sup>:

- **Completo:** para ello requiere todos los patrones necesarios para entrenar al modelo y que este formule predicciones precisas. Por ejemplo, si queremos entrenar un modelo que depende de datos de las operaciones de los contribuyentes (compras y ventas), el entrenamiento se verá afectado si a algunas transacciones les falta información esencial (fecha, cliente e importe), o no podemos discriminar entre las notas de débito o crédito y las facturas originales emitidas.
- **Únicos:** si tiene muchos duplicados, no va a aprender con exactitud. Por ejemplo, si queremos entrenar un modelo que depende de datos de los contribuyentes (ingresos, bienes registrables y consumos relevantes), el entrenamiento se verá afectado si algunas transacciones no pueden ser asignadas unívocamente a un sujeto por estar identificadas con diferentes números de inscripción (un mismo sujeto es informado alternativamente según la fuente o el momento con su documento de identidad, clave de identificación fiscal, cédula de identidad provincial o número de inscripción en oficinas de rentas subnacionales).
- **Actuales y vigentes:** si los datos pierden actualidad, se tornan irrelevantes, por lo que es necesario definir acciones en caso de caducidad. Por ejemplo, si queremos entrenar un modelo que depende de datos del patrimonio de los contribuyentes (inmuebles, automóviles, embarcaciones y aeronaves), el entrenamiento se verá afectado si a algunas transacciones les falta información reciente o no están registradas las últimas transferencias de dominio de los bienes registrables.
- **Tener un rango válido:** los datos deben cumplir con esquemas y principios predefinidos, como el tipo y el rango, para garantizar su integridad y utilidad. Ello asegura que estos datos se encuentren dentro de un rango esperado, lo que facilita su análisis y procesamiento de manera eficiente. Por ejemplo, si queremos entrenar un modelo que depende de datos de ingresos y gastos de los contribuyentes (acreditaciones bancarias, consumos relevantes y remuneraciones percibidas), el entrenamiento se verá afectado si en algunas transacciones se importa incorrectamente el dato por error en el formato, en la posición de la coma o por expresión en diferentes tipos de monedas o, incluso, si no se diferencia a los débitos de los créditos (o a las compras de las ventas).
- **Exactos:** en este punto se focaliza en el contenido del dato; por ejemplo, debemos tener cuidado en la captura de la fecha correcta o en la cantidad precisa de unidades vendidas.

- **Uniformes y concordantes:** la información de este tipo genera complicaciones en el modelo y su función; por ejemplo, la apreciación de un mismo contribuyente con diferentes denominaciones o con valores discordantes en diferentes campos de los datos como sus dominios o su actividad económica.

## b) *Machine Learning*<sup>[16]</sup>

Se necesita usar dichos datos para tomar decisiones y aquí entran en juego, una vez más, las tecnologías de IA<sup>[17]</sup>. A través de la *Machine Learning* (ML) se permite ejecutar tareas de forma autónoma y mejorar su rendimiento a través de la experiencia y la exposición a datos. Kevin Ashley explica este proceso inductivo en los siguientes términos:

*"Los algoritmos de machine learning identifican patrones en los datos, resumen esos patrones en un modelo<sup>[18]</sup> y utilizan ese modelo para identificar los mismos patrones en nuevos datos."*<sup>[19]</sup>

En tecnologías de IA las máquinas no toman decisiones, sino que las personas que las diseñan son las que influyen en la recopilación de datos, en el entrenamiento de los modelos y quienes deciden cómo usar las predicciones o prescripciones que resultan de la aplicación de los algoritmos.

Las técnicas de *Machine Learning* no solo se emplean para detectar anomalías e identificar patrones transaccionales difíciles de reconocer, sino que también permiten analizar y advertir relaciones entre personas y entidades sospechosas.<sup>[20]</sup>

Ahora bien, para lograr mayor claridad expositiva es necesario precisar ciertos conceptos fundamentales de la temática en trato.

El aprendizaje profundo (AP) y el aprendizaje automático suelen usarse indistintamente, aunque existen diferencias importantes. El AA, el AP y las redes neuronales artificiales (RNA) son subcampos de la IA. Sin embargo, las redes neuronales son un subcampo del aprendizaje automático, y el aprendizaje profundo es, a su vez, un subcampo dentro de las redes neuronales.

**1. El aprendizaje automático clásico**, o 'no profundo', depende en mayor medida de la intervención humana. Los expertos determinan el conjunto de características necesarias para diferenciar los datos de entrada, lo que generalmente requiere conjuntos de datos más estructurados. Se divide en tres categorías:

- **Aprendizaje supervisado:** utiliza conjuntos de datos etiquetados para entrenar algoritmos que clasifican información o predicen resultados con precisión. Durante el proceso, el modelo ajusta sus ponderaciones hasta lograr la mejor correspondencia, minimizando problemas de sobreajuste o subajuste mediante validación cruzada.

- **Aprendizaje no supervisado:** emplea algoritmos capaces de analizar y agrupar conjuntos de datos no etiquetados, formando clústeres. Estos modelos identifican patrones ocultos sin intervención humana.

- **Aprendizaje semisupervisado:** combina elementos de los enfoques anteriores. Utiliza un pequeño conjunto de datos etiquetados para guiar el modelo en la clasificación de un conjunto de datos más grande no etiquetado, lo que resulta útil cuando no hay suficientes datos etiquetados para entrenar un modelo supervisado.

**2. La red neuronal artificial** es un modelo inspirado en el funcionamiento del cerebro. Se compone de capas de nodos interconectados: una capa de entrada, una o más capas ocultas y una capa de salida. Cada nodo tiene un peso y un umbral asociado; si la salida de un nodo supera el umbral, se activa y transmite información a la siguiente capa. De lo contrario, no lo hace.

**3. El aprendizaje profundo** (o *deep learnig*) se refiere al número de capas de una red neuronal. Una red con más de tres capas -incluyendo entrada y salida- se considera un modelo de aprendizaje profundo, mientras que una con solo tres capas es una red neuronal básica.

El aprendizaje automático profundo puede utilizar conjuntos de datos etiquetados (aprendizaje supervisado), pero también procesar datos no estructurados sin etiquetar, como texto o imágenes. En este caso, el modelo determina automáticamente las características que diferencian las categorías de datos, reduciendo la intervención humana y permitiendo el uso de grandes volúmenes de datos. Como señala Lex Fridman en su conferencia en el Instituto de Tecnología de Massachusetts (MIT), el aprendizaje profundo puede considerarse '*aprendizaje automático escalable*'.<sup>[21]</sup>

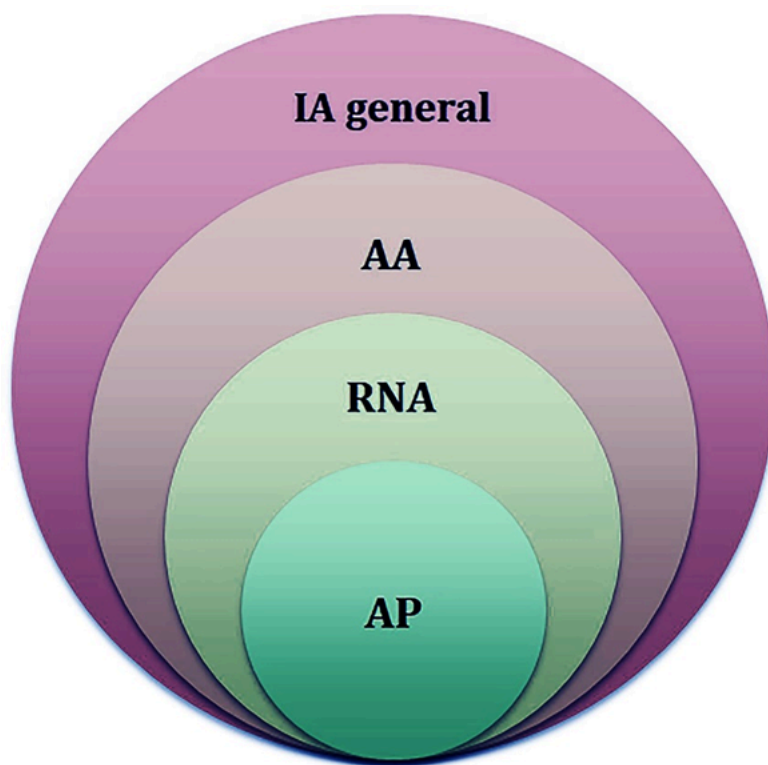


Gráfico de elaboración propia sobre la explicación expuesta

#### IV - EL IA EN BASE A MODELOS DE RECONOCIMIENTO SITUACIONAL

¿Qué tipo de modelos aquí nos interesa? Aquellos que se basan en **reconocimiento situacional**. Este concepto, con raíces en la filosofía estratégica de Sun Tzu<sup>[22]</sup>, se refiere a la capacidad de comprender y percibir con precisión lo que sucede en el entorno inmediato, además de anticipar y prepararse para eventos futuros.

En este sentido, se han desarrollado diversas soluciones de IA aplicadas a modelos avanzados de análisis tributario. Ejemplo de ello es la gestión del impuesto al valor agregado (IVA) y el análisis de riesgo, que se ejecutan regularmente para prevenir el fraude fiscal<sup>[23]</sup>. En un contexto caracterizado por grandes volúmenes de datos, capturas instantáneas de información (facturas electrónicas y formularios) y esquemas de defraudación que evolucionan rápidamente, la IA puede desempeñar un papel fundamental mediante un modelo de reconocimiento situacional. Este enfoque ha sido probado en entornos de alto estrés, en los que se requiere evaluar datos masivos de manera ágil y precisa.<sup>[24]</sup>

Los algoritmos de IA están diseñados y entrenados para analizar datos provenientes de diversos sensores con el objetivo de identificar amenazas y fortalecer la conciencia situacional. Este principio fundamental -la capacidad de percibir, comprender y anticipar con precisión los acontecimientos- es la base de procesos clave como la toma de decisiones y la ejecución de acciones estratégicas (*OODA loop*).<sup>[25]</sup>

Las metodologías de IA basadas en reconocimiento situacional constituyen el eje de aplicaciones militares, incluyendo aviones de combate, coordinación de fuerzas terrestres en operaciones activas y vuelos espaciales tripulados. En la esfera financiera, el flujo de datos económicos procesados en un contexto tributario transaccional, en el que el fraude debe ser detectado en tiempo real, también demanda técnicas de IA con capacidades similares.

Otro ejemplo ilustrativo es el uso de sensores IoT<sup>[26]</sup> en la prevención de la trata de personas. Estos sensores combinan el rastreo de ubicación en tiempo real con la detección de movimiento y proximidad, complementando su análisis con datos adicionales que pueden alertar a las fuerzas del orden sobre actividades sospechosas. La colocación estratégica de sensores facilita la detección, la identificación y el rescate de víctimas. Asimismo, el IoT, junto con tecnologías de IA y aprendizaje automático, puede analizar patrones de comportamiento y predecir posibles focos de trata, además de identificar a los perpetradores más frecuentes.

Finalmente, la conexión lógica entre estos elementos facilita la transmisión de información y la integración de recursos. En el ámbito tributario, el Registro Único Tributario -como identificador del contribuyente- y la factura electrónica -como mecanismo de control de ingresos y gastos- junto con el sistema financiero, que registra movimientos de recursos, constituyen los pilares para identificar en tiempo real operaciones sospechosas. De este modo, las autoridades contarían con pruebas suficientes para sancionar contribuyentes que operen como EFOS y/o EDOS<sup>[27]</sup>.

#### V - LA IA EN EL DERECHO COMPARADO

En Estados Unidos se desarrolló *Shape Security*<sup>[28]</sup>, una herramienta informática basada en IA y *Machine Learning*. Según su sitio web, los atacantes pueden parecer prácticamente idénticos a los usuarios legítimos al secuestrar dispositivos, simular comportamientos humanos y utilizar identidades robadas. Debido a la rápida evolución de sus técnicas, resulta casi imposible para las aplicaciones o incluso para las personas diferenciar lo genuino de lo fraudulento. Esta aplicación permite detectar y prevenir ataques y fraudes informáticos en tiempo real.



Por su parte, en Inglaterra, la policía emplea Connect, un sistema que analiza miles de millones de datos de transacciones financieras para identificar correlaciones y patrones de operaciones sospechosas.

En Italia, se implementó el sistema VERA<sup>[29]</sup> (Verificación de Informes Financieros), diseñado para combatir la evasión fiscal. Este algoritmo reconstruye los datos de los contribuyentes e identifica perfiles de riesgo, permitiendo una fiscalización más efectiva.

La Administración Tributaria de Noruega (NTA) ya utiliza técnicas de análisis de datos y aprendizaje automático para mejorar la eficiencia en la selección de casos de inspección. Esto facilita determinaciones tributarias de alto impacto fiscal e incluso la posibilidad de denuncias penales cuando corresponda.

En Alemania, la entidad reguladora BaFin publicó en 2022 el informe *Aprendizaje automático en modelos de riesgo*, centrado en la aplicación de técnicas de *Machine Learning*. Reconoció su utilidad para que las instituciones financieras identifiquen riesgos, pero advirtió que la 'explicabilidad' de estos métodos es un aspecto crucial. Además, enfatizó la necesidad de armonizar los requisitos de supervisión para estos modelos en toda Europa y en todos los sectores: *'deberían armonizarse en toda Europa y ser uniformes en todos los sectores'*<sup>[30]</sup>

En el ámbito de la fiscalización, la Receita Federal do Brasil desarrolló, junto con universidades nacionales, el proyecto HARPIA (*Risk Analysis and Applied Artificial Intelligence*). Este sistema detecta anomalías en operaciones financieras y ayuda a los fiscalizadores a identificar transacciones sospechosas mediante la visualización gráfica de datos históricos de importaciones y exportaciones. También emplea cadenas de Markov para asistir a los importadores en el registro y clasificación de productos, evitando duplicidades y asegurando una validación más eficiente en un determinado dominio. Se trata de procesos complejos que pueden generar cruces de información con los llamados "archivos digitales", que son solicitados por el auditor fiscal de la Secretaría de Ingresos Federales -SRF- a través del sistema de validación y autenticación de archivos digitales -SVA-<sup>[31]</sup>

Desde 2016, Brasil ha incorporado la inspección selectiva inteligente basada en Big Data y análisis de datos para controlar el IVA (ICMS) y los impuestos sobre vehículos, optimizando el proceso de fiscalización tributaria.<sup>[32]</sup>

## VI - LA IA APLICADA EN LA ADMINISTRACIÓN TRIBUTARIA ARGENTINA

A través de la [resolución general 5329](#) dictada por la Administración Federal de Ingresos Públicos (AFIP<sup>[33]</sup>), con fecha de publicación en el Boletín Oficial el 13/2/2023<sup>[34]</sup>, se puso en vigencia la primera etapa del "Programa de Monitoreo Fiscal" con fundamento en el desarrollo de nuevas modalidades de control para inferir anticipadamente la magnitud de las obligaciones fiscales, implicando un proceso de cambio y modernización.

Dicho programa, según se expresa en la norma, controlará (por el momento solo a personas jurídicas) en tiempo real las declaraciones juradas que presenten los contribuyentes y responsables, dando como resultado un mayor control de las transacciones concertadas y/o perfeccionadas, reduciendo las posibilidades de evasión<sup>[35]</sup>. El artículo 2 de dicha resolución establece:

*"El referido programa se instrumentará mediante una Matriz de Riesgo de Indicadores Fiscales, que determinará un índice aplicable para efectuar los controles pertinentes al momento de la presentación de las declaraciones juradas de cada período fiscal -según el tipo de impuesto de que se trate- y que será confeccionado a partir de la totalidad de las declaraciones juradas presentadas en los últimos doce (12) meses para los impuestos de período fiscal mensual y en los últimos tres (3) años para los impuestos con período fiscal anual".*

En otras palabras, a través de este acto administrativo, se le da el marco jurídico para la aplicación de un software que "...controlará de manera sistémica, instantánea y permanente las declaraciones juradas presentadas por los contribuyentes y responsables"<sup>[36]</sup>

Asimismo, en diversos medios de comunicación han señalado aspectos específicos de su funcionamiento:

*'Respecto al funcionamiento, desde la AFIP detallaron que la nueva herramienta cruza automáticamente bases de datos de los contribuyentes y, al encontrar una falta, genera automáticamente una comunicación con el contribuyente y el reclamo en el organismo'*<sup>[37]</sup>

Tanto en el Plan Estratégico 2021-2025 como en el Proyecto de Plan de Gestión 2023 de la AFIP se destaca el valor analítico del uso de técnicas como *Data Mining*, modelos predictivos, clasificación y decisión, Ciencia de Datos e IA. La automatización de ciertas tareas, aunque implique un grado de deshumanización, ofrece beneficios significativos y se encuentra en línea con tendencias globales adoptadas por administraciones fiscales de distintos países.

## VII - LA COMPATIBILIDAD DE LA IA CON DERECHOS FUNDAMENTALES

La IA representa una gran oportunidad para modernizar la Administración Tributaria mediante su digitalización. Sin embargo, esta transformación debe ir acompañada de una sólida protección de los derechos humanos de los ciudadanos. Nuestra [Constitución Nacional](#), como ocurre en otros ordenamientos del derecho comparado<sup>[38]</sup>, reconoce la protección de la correspondencia y otros datos personales que hacen a la privacidad y la intimidad de los contribuyentes [arts. 18 y 75, inc. 22), CN; art. 17 del Pacto Internacional de Derechos Civiles y Políticos, y art. 11.2 de la Convención Americana sobre Derechos Humanos].

Tal como lo ha dicho el Supremo Tribunal Constitucional Español<sup>[39]</sup>, la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona.

La Administración Tributaria cuenta con amplios poderes para recolectar, almacenar y proceder al tratamiento de información relacionada con sus potestades fiscales<sup>[40]</sup>, es decir, datos tributarios<sup>[41]</sup>. Las declaraciones juradas, las manifestaciones y los informes que los responsables o terceros presenten ante aquella, las actuaciones administrativas labradas en su ámbito, las ejecuciones fiscales que promuevan sus autoridades y las demandas contenciosas o por repetición que articulen los interesados deben ajustarse a las disposiciones contenidas en la [ley 11683](#), con modificaciones introducidas por el

decreto 1334/1998 y la ley 25239, como asimismo a las normas de la ley 19549, modificada por las leyes 21686 y 25344, y por el decreto 1023/2001.

Asimismo, la ley 25326 de protección de datos personales y su reglamentación resguardan la privacidad de la información personal. Esta normativa se complementa con la "Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público" [aprobada por la Disp. (DNPDP) 7/2008, del 22/8/2008], la resolución 40/2018, del 4 de julio de 2018 sobre la Política Modelo de Protección de Datos Personales para Organismos Públicos, y el dictamen 149/2007 de la Dirección Nacional de Protección de Datos Personales.

Por otro lado, la ley de procedimiento tributario establece el secreto fiscal como un mecanismo legal para proteger la información económica y patrimonial de los contribuyentes dentro de la AT, delimitando el artículo 101, en sus párrafos quinto y sexto, los casos en los que esta protección no aplica.

La digitalización de la Administración Tributaria debe fundamentarse en los principios de dignidad, identidad y vulnerabilidad algorítmica, los cuales derivan de la dignidad e identidad digital de las personas en entornos virtuales. Es esencial evitar la discriminación algorítmica<sup>[42]</sup> y garantizar que el tratamiento de datos sensibles, protegidos por el secreto fiscal, cumpla con los más altos estándares de seguridad, transparencia y explicabilidad en los procesos automatizados. Asimismo, el entrenamiento de modelos de IA debe alinearse con principios éticos, asegurando una gestión equitativa y confiable de la información.

El sistema de protección debe basarse en ciertos principios rectores<sup>[43]</sup>:

- **Prevención y precaución:** son principios que cumplen funciones distintas, pero comparten un mismo objetivo, esto es, la necesidad de actuar antes de que se produzca un daño. En términos generales, se aplican a diferentes tipos de riesgos: la precaución frente a riesgos potenciales y la prevención ante riesgos verificados.

El principio precautorio en el ámbito de la IA, al igual que en el derecho ambiental, surge ante la ausencia absoluta de certeza científica sobre la inexistencia de riesgos. Cuando un sistema de IA puede impactar en derechos fundamentales de las personas -como la salud, la libertad, la igualdad y la no discriminación, o la seguridad-, no debería emplearse si se presentan las siguientes condiciones:

- i) Código fuente cerrado o existencia de un sistema en el que se comprenden los datos de entrada y los resultados, pero no el proceso subyacente (fenómeno conocido como 'caja negra').
- ii) Falta de trazabilidad algorítmica, lo que impide conocer el funcionamiento interno del sistema.
- iii) Imposibilidad de garantizar un mecanismo seguro de contención, como un 'botón de apagado' para detener el sistema en caso necesario.
- iv) Uso de distinciones discriminatorias en cualquier fase del diseño, desarrollo o aplicación, vulnerando los principios de igualdad y no discriminación.

En este contexto, se plantea la existencia de una 'categoría sospechosa algorítmica', es decir, un criterio de clasificación que podría generar impactos injustos o discriminatorios.

- **Autodeterminación algorítmica:** se trata de asegurar el "libre desarrollo de la personalidad" a partir de reconocer la autodeterminación informativa que se orienta a garantizar el derecho a elegir -asociado a la libertad de información-, el "derecho a saber", al "conocimiento" y a la "autorregulación de la información".<sup>[44]</sup>

- **Transparencia algorítmica y principio de imparcialidad del validador:** cuando se pretende utilizar sistemas de IA en ámbitos sensibles como la salud, la libertad, la seguridad u otros derechos fundamentales, es esencial que su diseño, desarrollo y uso garanticen la ausencia de *cajas negras* y la identificación de posibles fallas de arquitectura que puedan generar daños o lesiones.

Para abordar el fenómeno de las *cajas negras*, es importante recordar que los sistemas de IA están diseñados para maximizar resultados y optimizar el procesamiento de información y datos. Sin embargo, cuando están en juego derechos fundamentales -como la salud, la vida, la libertad, la privacidad y la libertad de expresión-, es clave que los resultados intermedios del sistema sean validados.

Esto implica que el razonamiento o las estructuras de razonamiento que conducen a decisiones y predicciones deben someterse a un proceso que consta de tres grandes fases<sup>[45]</sup>:

- a) Verificación.
- b) Validación.
- c) Evaluación.

Estas etapas son fundamentales para garantizar la calidad y transparencia de los procesos algorítmicos, asegurando que los sistemas de IA operen de manera ética y respeten los derechos de las personas.

Incluso, es indispensable que las autoridades públicas intervengan en el proceso y se obligue legalmente a que esto ocurra, máxime cuando se están desarrollando algoritmos que impactan en la vida, seguridad, libertad y salud de las personas.

- **Trazabilidad de la IA:** la trazabilidad, también conocida como *rastreabilidad*, es la capacidad de seguir la historia, aplicación o ubicación de una entidad a través de registros documentados. Una IA basada en un enfoque de derechos humanos debe garantizar la transparencia en cada paso del proceso técnico, desde su inicio hasta su conclusión. Es fundamental que el proceso de toma de decisiones de los algoritmos inteligentes sea comprensible y trazable, asegurando así el máximo acceso a la información.

- **Derecho de acceso a la información algorítmica:** tanto el Estado como las entidades públicas no estatales, ya sea directamente o mediante terceros, tienen la responsabilidad de garantizar el acceso a la información sobre los sistemas que diseñan, desarrollan o utilizan basados en IA o

algoritmos inteligentes. Esto incluye cualquier tipo de máquina o robot inteligente y su sistema de procesamiento de datos, asegurando la máxima transparencia en el uso de estas tecnologías.

- **Principio de no discriminación algorítmica:** los algoritmos inteligentes deben ser diseñados e implementados respetando el principio de no discriminación. Esto significa que los sistemas de IA deben evitar procesar información con sesgos que puedan generar desigualdades o injusticias. La equidad en el tratamiento de datos es fundamental para garantizar el uso responsable y ético de la IA.

A nivel internacional, la Unión Europea ha desarrollado un reglamento 2024/1689 del Parlamento europeo y del consejo (13/6/2024) por el que se establecen normas armonizadas en materia de IA. Se enfoca en la seguridad, la privacidad y la no discriminación en el uso de IA, y la clasifica por niveles de riesgo. La IA se categoriza en cuatro niveles: riesgo inaceptable (prohibido), alto riesgo (regulado estrictamente), medio riesgo y mínimo riesgo. Asimismo, exige que los sistemas de IA sean auditables y comprensibles para evitar sesgos y garantizar su trazabilidad.

## VIII - CONCLUSIÓN

La incorporación de la IA en la Administración Tributaria representa una evolución fundamental en la lucha contra la evasión fiscal, ofreciendo herramientas avanzadas para la identificación y fiscalización de prácticas de evasión fiscal. A lo largo del análisis presentado, se ha destacado cómo el uso de técnicas como el aprendizaje automático y el reconocimiento situacional permite optimizar la recaudación, mejorar el cumplimiento tributario y fortalecer la transparencia del sistema fiscal.

Sin embargo, esta transformación no está exenta de desafíos. La implementación de IA en la fiscalización debe equilibrarse con el respeto a los principios de legalidad, privacidad y protección de datos personales, evitando que los ciudadanos sean tratados indiscriminadamente como evasores. La recopilación y el procesamiento de datos a gran escala generan preocupaciones legítimas sobre el uso indebido de información, el riesgo de sesgos algorítmicos y la posible vulneración de derechos fundamentales.

El derecho comparado nos muestra diversas experiencias internacionales en las que la IA ha sido aplicada con éxito en la lucha contra la evasión fiscal. Desde el desarrollo de algoritmos predictivos en Estados Unidos hasta la aplicación de herramientas inteligentes en Brasil, la transformación digital de las administraciones tributarias ha demostrado mejorar la eficiencia recaudatoria y reducir las oportunidades de fraude. Estos avances ofrecen un modelo útil para su implementación en Argentina, en el que la Agencia de Recaudación y Control Aduanero ha comenzado a adoptar tecnologías similares a través del Programa de Monitoreo Fiscal.

No obstante, la efectividad de estas medidas dependerá no solo de su capacidad tecnológica, sino también de su correcta reglamentación y supervisión. Para que la IA funcione como un recurso legítimo en la Administración Tributaria, es fundamental establecer parámetros claros que garanticen la transparencia en el uso de datos, la auditabilidad de los modelos y la equidad en los procedimientos de fiscalización. La normativa debe definir con precisión los límites de su aplicación, evitando que el avance tecnológico se convierta en un instrumento de control excesivo o discriminación.

En este contexto, la digitalización de la Administración Tributaria representa una oportunidad única para fortalecer la eficiencia del sistema fiscal sin comprometer los derechos individuales. La clave radica en garantizar que la implementación de IA responda a un modelo ético, en el que la automatización de procesos esté acompañada de principios de equidad y justicia tributaria. Solo así se podrá lograr un equilibrio entre innovación tecnológica y garantías legales, asegurando que el progreso en la fiscalización fiscal contribuya al bienestar económico y social sin afectar la dignidad y privacidad de los ciudadanos.

## Florencia Ungra

Maestranda en Derecho Penal en la Universidad Torcuato Di Tella. Abogada egresada con honores de la Universidad Católica de La Plata (UCALP), distinguida con los premios al mejor promedio de la Facultad de Derecho y de la Universidad. Profesora de Derecho Penal Parte General y Litigación en la UCALP, además de investigadora en la misma institución. Auxiliar letrada de la Sala II de la Cámara de Apelaciones y Garantías del Departamento Judicial de Quilmes, Provincia de Buenos Aires. Autora y coautora de diversos artículos y libros especializados en Derecho Penal y Procesal Penal.

---

[1] Carranza Torres, Luis R.: "Derecho tributario: de la teoría a la práctica" - Ed. Legis Argentina - Bs. As. - 2006 - pág. 27

[2] Discurso ante los líderes del G7 - 14/6/2024

[3] "Art. 4 - El Gobierno Federal provee a los gastos de la Nación con los fondos del Tesoro Nacional, formado del producto de derechos de importación y exportación de las aduanas, del de la venta o locación de tierras de propiedad nacional, de la renta de correos, de las demás contribuciones que equitativa y proporcionalmente a la población imponga el Congreso General, y de los empréstitos y operaciones de crédito que decreta el mismo Congreso para urgencias de la Nación o para empresas de utilidad nacional"

[4] Wagner, Adolph: "Traité de la science des finances" - París - 1909

[5] Villegas, Héctor B.: "Régimen penal tributario argentino" - Ed. Depalma - Bs. As. - pág. 5

[6] Gómez de la Torre, Ignacio B. y Ferré Olivé, Juan C.: "Todo sobre el fraude tributario" - Ed. Praxis - Barcelona - 1994 - pág. 2

[7] Edwards, Carlos E.: "Régimen penal tributario" - Ed. Astrea - Bs. As. - 2000 - págs. 17/8

[8] González Cao, Rodrigo L.: "Inteligencia Artificial, Gobierno Abierto y Secreto Fiscal en las Administraciones Tributarias" - CEAT. Disponible en <https://www.economicas.uba.ar/extension/wp-content/uploads/inteligencia-artificial-gobierno-abierto-y-secreto-fiscal.pdf>. Consultado el 22/4/2025



[9] "Five components that artificial intelligence must have to succeed". Véase en <https://www.bloomberg.com/professional/blog/five-components-artificial-intelligence-must-succeed/>. Consultado el 16/5/2025

[10] Cuatrecasas Monforte, Carlota: "La Inteligencia Artificial como herramienta de investigación criminal" - LL - Bs. As. - 2022

[11] Calaña Xavier, Otávio; Ramos Pires, Sandrerley; Carvalho Marques, Thyago y da Silva Soares, Anderson: 'Tax evasion identification using open data and artificial intelligence'. Véase en <https://www.scielo.br/j/rap/a/5q38f9RdbQYSrZXF8zfDJqv/?format=pdf&lang=en>. Consultado el 20/4/2025

[12] Aznar, Carlos M. y Fernández, Néstor J.: "La Inteligencia Artificial como herramienta de investigación en los delitos tributarios", en <https://caept.org.ar/wp-content/uploads/2023/10/La-inteligencia-artificial-como-herramienta-de-investigacio%CC%81n-en-los-delitos-tributarios-version-corr.pdf>. Consultado el 4/5/2024

[13] Mielnik, David: "Análisis computacional del Derecho Argentino" - Universidad Torcuato Di Tella - Escuela de Derecho - Revista Argentina de Teoría Jurídica (RATJ) - Vol. 23 - N° 1 - diciembre/2022 - págs. 6/7

[14] Los sesgos se refieren a la tendencia de los algoritmos a tomar decisiones incorrectas o injustas debido a datos sesgados o algoritmos diseñados con prejuicios humanos. Estos sesgos pueden generar resultados discriminatorios, perpetuar estereotipos o dificultar la participación de ciertos grupos en la sociedad

[15] González Cao, Rodrigo L.: “Inteligencia Artificial, Gobierno Abierto y Secreto Fiscal” - Centro de Estudios en Administración Tributaria - 2024 - págs. 26/8. Disponible en <https://www.economicas.uba.ar/extension/wp-content/uploads/inteligencia-artificial-gobierno-abierto-y-secreto-fiscal.pdf>. Consultado el 16/5/2025

[16] El ML es, en esencia, una rama de la IA que permite a las máquinas aprender de la experiencia, imitando en cierta forma el proceso de aprendizaje humano. En lugar de seguir instrucciones rígidas para cada tarea, los algoritmos de ML analizan grandes volúmenes de datos, identifican patrones y ajustan sus modelos para mejorar continuamente su desempeño

[17] González Cao, Rodrigo L.: “Inteligencia Artificial, Gobierno Abierto y Secreto Fiscal” - Ob. cit. en nota 15 - pág. 14

[18] “La representación matemática de las relaciones entre las variables que surgen de los datos a los que el algoritmo es expuesto”. Grus, Joel: “Data Science from Scratch: First Principles with Python” - O’Reilly Media - 2015 - págs. 141/2

[19] Ashley, Kevin D.: "Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age" - Cambridge University Press - 2017 - pág. 234

[20] Forensic: “The case for artificial intelligence in combating money laundering and terrorist financing. A deep dive into the application of machine learning technology” - Deloitte - 2018.

[21] Fridman, Lex: "Deep Learning Basics: Introduction and Overview" - Véase en <https://www.youtube.com/watch?v=Q5xevoRL95U> - Consultado el 4/5/2025

[22] Sun Tzu fue un general, estratega militar y filósofo de la antigua China. El nombre por el que lo conocemos es en realidad un título honorífico que significa "Maestro Sun". Su nombre de nacimiento era Sun Wu y fuera de su familia era conocido por su nombre de cortesía: Changqing

[23] Ainsworth, Richard T., Alwohaibi, Musaad; Cheetham, Mike y Tirand, Camile: "A VATCoin Solution to MTIC Fraud: Past Efforts, Present Technology, and the EU's 2017 Proposal" - Boston University School of Law - Boston - 2018

[24] Seco, Antonio y Muñoz Miranda, Andrés: “Panorama del uso de soluciones digitales innovadoras en la política y la gestión fiscal” - Documento para discusión IDB-DP-602 - BID - Washington, D.C. - 2018. Disponible en: <https://publications.iadb.org/es/publications/spanish/viewer/Panorama-del-uso-de-las-tecnolog%C3%ADas-y-soluciones-digitales-innovadoras-en-la-pol%C3%ADtica-y-la-gesti%C3%B3n-fiscal.pdf> - Consultado el 16/5/2025

[25] El ciclo OODA (Observar, Orientar, Decidir, Actuar) es un modelo de toma de decisiones desarrollado por el coronel John Boyd, que se utiliza para tomar decisiones rápidas y eficaces en entornos dinámicos y complejos. El ciclo se enfoca en la velocidad y la flexibilidad en la toma de decisiones, permitiendo a los individuos y organizaciones adaptarse rápidamente a los cambios.

[26] “¿Qué es internet de las cosas (IoT)?” - SAP. Véase en:  
[https://www.sap.com/latinamerica/products/technology-platform/what-is-  
 iot.html#:~:text=%C2%BFQu%C3%A9%20es%20internet%20de%20las%20cosas%20\(IoT\)?,%E2%80%93desde%20y%20hacia%20otras%20cosas%20y%20](https://www.sap.com/latinamerica/products/technology-platform/what-is-iot.html#:~:text=%C2%BFQu%C3%A9%20es%20internet%20de%20las%20cosas%20(IoT)?,%E2%80%93desde%20y%20hacia%20otras%20cosas%20y%20)  
 Consultado el 22/4/2025

[27] EFOS: Empresas que facturan operaciones simuladas. EDOS: Empresas que deducen operaciones simuladas

[28] “F5 Distributed Cloud Bot Defense”. Véase en <https://www.shapesecurity.com/solutions>. Consultado el 20/5/2025

[29] “Nasce VeRa, l'algoritmo per fermare l'evasione fiscale: 'Così creiamo le liste dei contribuenti anomali’”. Véase en <https://www.fanpage.it/innovazione/tecnologia/nasce-vera-lalgoritmo-per-fermare-levasione-fiscale-cosi-creiamo-le-liste-dei-contribuenti-anomali/>. Consultado el 16/5/2025

[30] Véase en [https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2022/fa\\_bj\\_2202\\_Maschinelles\\_Lernen\\_en.html](https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2022/fa_bj_2202_Maschinelles_Lernen_en.html). Consultado el 30/4/2025



- [31] Aznar, Carlos M. y Fernández, Néstor J.: "La Inteligencia Artificial como herramienta de investigación en los delitos tributarios" - Ob. cit. en nota 12
- [32] Ossandón Cerda, Francisco: "Inteligencia Artificial en las Administraciones Tributarias: oportunidades y desafíos" - Centro de Estudios Tributarios - Chile
- [33] En la actualidad se denomina Agencia de Recaudación y Control Aduanero (ARCA), organismo que tiene a su cargo la recaudación de impuestos, el control del comercio exterior y el cumplimiento de las obligaciones tributarias de los contribuyentes en materia impositiva, aduanera y previsional
- [34] ARCA - Biblioteca Electrónica. Véase en: <https://biblioteca.afip.gob.ar/search/query/norma.aspx?p=t:RAG/n:5329/o:3/a:2023/f:10/02/2023>. Consultado el 10/5/2025
- [35] Rubín, Santiago G.: 'AFIP: Inteligencia Artificial para el control de evasores' - ERREPAR - 25/4/2023. Véase en <https://documento.errepar.com/actualidad/afip-inteligencia-artificial-para-controlar-evasores>. Consultado el 16/5/2025
- [36] Cfr. art. 1, RG (AFIP) 5329
- [37] "Inteligencia Artificial: cómo funciona la nueva herramienta de la AFIP que ya le permitió recaudar \$ 4.500 millones" - iProfesional - 20/1/2022. Véase en <https://www.iprofesional.com/impuestos/355984-inteligencia-artificial-como-funciona-la-herramienta-de-la-afip>. Consultado el 19/5/2025
- [38] Art. 18.4: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos, y el pleno ejercicio de sus derechos" (Constitución española, 1978: 5)
- [39] Sent. 2564/1993
- [40] Art. 36, L. 11683, conf. D. 821/1998 y modif.
- [41] Toda aquella información referida a personas físicas o de existencia ideal determinadas o determinables, que se relacione con los aspectos fiscalmente relevantes de su composición patrimonial o su conducta
- [42] También conocida como *sesgo algorítmico*, se refiere al fenómeno en el cual los algoritmos de IA y aprendizaje automático perpetúan o incluso amplifican los prejuicios y sesgos humanos existentes en los datos con los que son entrenados
- [43] Corvalán, Juan G.: "Inteligencia Artificial: retos, desafíos y oportunidades" - Prometea: la primera Inteligencia Artificial de Latinoamérica al servicio de la Justicia - Revista de Investigações Constitucionais - Curitiba - Vol. 5 - N° 1 - págs. 295/316 - jan.-abr./2018 - DOI: 10.5380/rinc.v5i1.55334. Disponible en [https://www.researchgate.net/publication/323786322\\_Inteligencia\\_artificial\\_retos\\_desafios\\_y\\_oportunidades\\_-\\_Prometea\\_la\\_primera\\_inteligencia\\_artificial\\_de\\_Latinoamerica\\_al\\_servicio\\_de\\_la\\_Justicia](https://www.researchgate.net/publication/323786322_Inteligencia_artificial_retos_desafios_y_oportunidades_-_Prometea_la_primera_inteligencia_artificial_de_Latinoamerica_al_servicio_de_la_Justicia). Consultado el 16/5/2025
- [44] Pitschas, Rainer: "Derecho administrativo de la Información" - In: Barnes, Javier (Ed.): "Innovación y Reforma en Derecho Administrativo" - 2a. ed. - Global Law Press - Sevilla - 2012 - págs. 226, 227 y 236
- [45] Ampliar en Palma Méndez, José T. y Marín Morales, Roque: "Inteligencia Artificial" - Ed. McGraw-Hill - España - 2008 - págs. 891 a 935