LA INTELIGENCIA ARTIFICIAL EN LA ADMINISTRACIÓN TRIBUTARIA MEXICANA. AVANCES Y DESAFÍOS EN MATERIA DE SEGURIDAD JURÍDICA

Carlos ESPINOSA BERECOCHEA[1]

SUMARIO

RESUMEN

La Inteligencia Artificial (IA) ha evolucionado de ser un instrumento de carácter recreativo a convertirse en un componente estratégico para la eficiencia en los ámbitos profesional y económico. En el contexto del derecho fiscal mexicano, su implementación por parte del Servicio de Administración Tributaria (SAT) refleja un esfuerzo por modernizar los mecanismos de gestión recaudatoria. Sus aplicaciones abarcan desde la optimización de los servicios al contribuyente, promoviendo el cumplimiento de las obligaciones fiscales, hasta el reforzamiento de estrategias de recuperación de créditos fiscales, la detección de esquemas de evasión y la evaluación de riesgos asociados a perfiles contributivos.

No obstante, estos avances plantean cuestionamientos en torno a la seguridad jurídica, principio fundamental en un Estado de Derecho. La automatización de decisiones fiscales y la potencial falta de transparencia en los algoritmos de evaluación de riesgo

ABSTRACT

Artificial Intelligence (AI) has evolved from a recreational tool to a strategic component for enhancing professional and economic efficiency. In the context of Mexican tax law, its implementation by the *Servicio de Administración Tributaria* (SAT) reflects an effort to modernize revenue collection mechanisms. Its applications range from improving taxpayer services —facilitating compliance with fiscal obligations— to strengthening strategies for tax debt recovery, detecting evasion schemes, and assessing risks associated with taxpayer profiles.

However, these advancements raise concerns regarding legal certainty, a fundamental principle in a rule-of-law state. The automation of tax-related decisions and the potential lack of transparency in risk-assessment algorithms could create uncertainty among taxpayers, blurring the traditional boundaries of the State's auditing powers. Consequently, it is imperative to analyze the regulatory impact of AI on the tax system,

[1] Licenciado, Maestro y Doctor en Derecho por la Universidad Panamericana, Maestro en Ciencias Jurídicas por dicha Universidad y catedrático de la misma. Miembro del Sistema Nacional de Investigadores SNII de CONACHYT, Nivel I.

podrían generar incertidumbre entre los contribuyentes, diluyendo los límites tradicionales de las facultades fiscalizadoras del Estado. En este sentido, es imperativo analizar el impacto normativo de la IA en el sistema tributario, asegurando que su adopción se apegue a los principios de legalidad, proporcionalidad y debido proceso, consagrados en la Constitución Política de los Estados Unidos Mexicanos y en los tratados internacionales en materia de derechos humanos.

PALABRAS CLAVE

Inteligencia Artificial. Derecho fiscal. SAT. Seguridad jurídica. Principios constitucionales.

ensuring its adoption adheres to the principles of legality, proportionality, and due process, as enshrined in the Mexican Constitution and international human rights treaties.

KEYWORDS

Artificial Intelligence. Tax law. SAT. Legal certainty. Constitutional principles.

I. INTRODUCCIÓN

El avance tecnológico, expresado mediante conceptos como la Inteligencia Artificial (IA) y el Aprendizaje Automático[2], ha dejado de ser un fenómeno exclusivo del ámbito académico o de la ciencia ficción, para convertirse en un componente estructural de la vida cotidiana. Su presencia se manifiesta en acciones aparentemente triviales —como interactuar con asistentes personales que ejecutan instrucciones verbales desde dispositivos móviles o computadoras—, así como en sistemas que recomiendan productos de consumo basados en nuestros hábitos, optimizan rutas de navegación o mejoran el rendimiento de tareas mediante el uso de herramientas como el *Chatbot* de IA desarrollado por *OpenAI*[3] o el recientemente presentado por *Deep Seek*[4].

No obstante, el alcance de la IA ha superado ya los límites del uso doméstico, comercial o profesional de los individuos. Su potencial ha sido desplegado en esferas altamente complejas, tales como la automatización de procesos robóticos en la industria automotriz, el seguimiento de mercancías en las cadenas de suministro o la detección temprana de diversos tipos de cáncer mediante algoritmos avanzados.

En este contexto, resulta lógico que las ventajas asociadas al uso de estas tecnologías no permanezcan confinadas al sector privado. Por el contrario, diversos gobiernos han co-

[2] Traducción del término *Machine Learning*, que es el que suele encontrarse en la literatura de la materia.

[3] *OpenAI*, basado en la arquitectura de aprendizaje profundo de lenguaje natural, conocido como "transformer", *https://openai.com/*, visitada el 12 de noviembre de 2024.

[4] Su equivalente chino, creado por Lian Wenfeng, *https://www.deepseek.com/*, visitada el 12 de febrero de 2025.

menzado a incorporarlas activamente en el ejercicio de sus funciones públicas. En materia de gestión de datos, por ejemplo, se recurre a la IA para organizar y analizar grandes volúmenes de información, optimizar procesos de toma de decisiones y automatizar tareas rutinarias. Se emplean algoritmos inteligentes para identificar patrones demográficos que faciliten el diseño de políticas públicas más eficaces. En materia de seguridad pública y justicia penal, la IA se aplica al análisis de video en tiempo real para el reconocimiento facial y la detección de comportamientos sospechosos en espacios públicos. En el ámbito de la infraestructura y el urbanismo, la inteligencia artificial se utiliza para procesar datos sobre movilidad y medio ambiente, optimizando con ello el diseño urbano, la gestión del tráfico y la eficiencia energética de las ciudades. Por último, en la atención al ciudadano, los gobiernos han incorporado *chatbots* y asistentes virtuales para mejorar el acceso a servicios públicos, agilizar respuestas a consultas frecuentes y facilitar trámites administrativos[5].

Como el lector podrá intuir, los beneficios que se derivan del uso de la IA trascienden la esfera del consumidor o del productor de bienes y servicios, alcanzando incluso a uno de los actores más relevantes del aparato estatal: la Secretaría de Hacienda y Crédito Público (SHCP), y específicamente, al órgano recaudador por excelencia, el Servicio de Administración Tributaria (SAT).

Es sabido que el sistema fiscal mexicano se basa, entre otros principios, en la autodeterminación del contribuyente, esto es, en su obligación de calcular y enterar las contribuciones a su cargo conforme a lo dispuesto por la legislación aplicable[6]. En esta lógica, al SAT le corresponde verificar que dicha determinación se haya realizado de manera correcta y oportuna.

Es precisamente en esta función donde el uso de la inteligencia artificial adquiere una relevancia creciente. Actualmente, el SAT emplea herramientas de IA tanto para asistir a los contribuyentes mediante *chatbots*[7], como para detectar posibles supuestos de evasión fiscal, por ejemplo, a través de la identificación de Comprobantes Fiscales Digitales por Internet (CFDI)[8] que respaldan operaciones inexistentes. Asimismo, se ha documentado el envío de propuestas de pago prellenadas a los causantes y la estimación de contribuciones

---

[5] CFR. Según una respuesta generada por *ChatGPT* de *OpenAI* (consulta realizada el 12 de noviembre de 2024), *OpenAI. ChatGPT*. Versión GPT-4. San Francisco: *OpenAI,* 2023. *https://chat.openai.com/chat*.

[6] Código Fiscal de la Federación. Artículo 6o. Las contribuciones se causan conforme se realizan las situaciones jurídicas o de hecho, previstas en las leyes fiscales vigentes durante el lapso en que ocurran.
Dichas contribuciones se determinarán conforme a las disposiciones vigentes en el momento de su causación, pero les serán aplicables las normas sobre procedimiento que se expidan con posterioridad.

[7] Asistente que se comunica con los usuarios a través de mensajes de texto, *https://bloo.media/blog/por-que-implementar-chatbot-en-tu-estrategia-de-marketing/*.

[8] Conocido en otras legislaciones como factura electrónica, *eticket* o *electronic invoice.*

a pagar por parte de determinados grupos económicos, con base en modelos predictivos y parámetros comparativos.

Cabe señalar que, desde la administración presidencial anterior, se sentaron las bases para una integración más agresiva de estas tecnologías al ámbito fiscal, a través de instrumentos como el "Programa Plan Maestro 2024 SAT. Atención al contribuyente, recaudación y fiscalización"[9], el cual vislumbra un espectro de aplicaciones que rebasa los casos anteriormente expuestos. Lo anterior cobra mayor relevancia al considerar que ya existe un andamiaje normativo que aparentemente otorga sustento jurídico a estas prácticas, aunque no sin generar preocupaciones sobre sus efectos en la seguridad jurídica de los contribuyentes.

Con la transición reciente en el Poder Ejecutivo, marcada por la llegada de una nueva titular del Poder Ejecutivo Federal, no se ha advertido un cambio en la expectativa gubernamental respecto al uso de la IA en la gestión tributaria. Por el contrario, la publicación del "Plan Maestro 2025"[10] reafirma la continuidad de esta estrategia.

Por ello, se vuelve imprescindible volver la mirada a principios fundamentales del Derecho, cuya vigencia no ha sido superada por el desarrollo tecnológico, sino que, por el contrario, adquiere renovada importancia. Uno de estos pilares es la seguridad jurídica, concebida como la expectativa razonable y fundada que tiene el gobernado respecto de la actuación de la autoridad. En este sentido, la seguridad jurídica exige que la ley delimite con precisión las facultades del poder público, estableciendo de manera clara y detallada los márgenes dentro de los cuales puede actuar. Dichas facultades constituyen un límite infranqueable: ninguna autoridad puede realizar actos que no le hayan sido expresamente conferidos por el orden jurídico.

En el ámbito fiscal, este principio adquiere particular relevancia. La creación de tributos debe observar estrictamente el principio de reserva de ley, lo cual implica que toda iniciativa legislativa en materia tributaria debe originarse en la Cámara de Diputados y ser revisada por la Cámara de Senadores. Cualquier desviación de este procedimiento implica una transgresión al orden constitucional y, por ende, la invalidez de la norma tributaria resultante[11].

Además, la Constitución exige que los tributos sean proporcionales y equitativos. Para salvaguardar tales principios y evitar potenciales excesos por parte de la autoridad administrativa, los elementos esenciales de las contribuciones —tales como el objeto, la base gravable y otros aspectos sustanciales— deben encontrarse definidos de manera clara en

[9] *https://www.gob.mx/cms/uploads/attachment/file/883360/PlaMaestro2024.pdf*, visitada el 12 de octubre de 2024.
[10] *https://www.gob.mx/sat/documentos/plan-maestro-2025-enero-2025*, visitada el 20 de febrero de 2025.
[11] Tesis P./J. 51/2002, *Semanario Judicial de la Federación y su Gaceta*, t. XVI, diciembre de 2002, p. 5, Registro Digital: 185420.

la ley. Solo así se garantiza que el contribuyente tenga certeza jurídica respecto de sus obligaciones fiscales, en congruencia con el principio de seguridad jurídica, al permitirle prever razonablemente la conducta de la autoridad fiscal conforme al marco normativo aplicable.

En ese sentido, podría sostenerse que, en el diseño tradicional de la relación tributaria, la seguridad jurídica se preservaba mediante la autodeterminación del tributo por parte del contribuyente, y el ejercicio acotado de las facultades de comprobación por parte de la autoridad. Esta, ante una posible discrepancia, debía ajustarse estrictamente a los cauces legales para modificar la determinación fiscal realizada por el particular, imponiendo —en su caso— los accesorios que correspondieran. No obstante, el propio sistema jurídico provee al contribuyente de una serie de medios de defensa para impugnar cualquier actuación de la autoridad que contravenga el marco normativo.

Sin embargo, el auge de la inteligencia artificial unido al uso intensivo de herramientas digitales y al manejo de grandes volúmenes de datos, ha modificado radicalmente esta concepción tradicional. Como se analizará más adelante, ha surgido una nueva lógica en la manera de concebir el cumplimiento de las obligaciones fiscales. Esta lógica, aunque mantiene como principio la autodeterminación del tributo, redefine las formas en que se conserva la contabilidad, se exhibe a la autoridad, se expiden comprobantes fiscales y se realiza la revisión por parte del fisco.

Nos encontramos así ante una nueva era de la seguridad jurídica, donde la administración, almacenamiento, tratamiento, transmisión y protección de los datos personales adquieren un papel central. La problemática ya no se limita a las implicaciones típicas de los delitos informáticos, sino que abarca riesgos sustantivos derivados de la posibilidad de que los datos del contribuyente —en manos propias o de la autoridad— puedan ser utilizados sin control adecuado, incluso por personas no facultadas jurídicamente para ello. Este fenómeno, aún poco explorado por la doctrina jurídica mexicana, demanda una atención prioritaria frente al avance inexorable de la tecnología.

II. EL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA Y LA INTELIGENCIA ARTIFICIAL

Desde el inicio de este trabajo se ha enfatizado que el propósito no es abordar la inteligencia artificial (IA) desde una perspectiva informática[12], ni mucho menos realizar una disertación sobre su base científica o estructural. El objetivo se centra, más bien, en analizar las implicaciones jurídicas que su aplicación ha generado —y continúa generando— en el ámbito tributario mexicano, particularmente a partir de la implementación de los programas

[12] Neologismo derivado de los vocablos información y automatización, sugerido por Philipe Dreyfus en 1962, siendo entonces el conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de decisiones. En Téllez Valdez, Julio, *Derecho Informático*, 2a. ed., México, Mc Graw Hill, 1998, p. 3.

institucionales denominados *Plan Maestro 2024* y *Plan Maestro 2025* del Servicio de Administración Tributaria (SAT), a los que ya se ha hecho referencia en el apartado introductorio.

Una vez delimitado este marco, es conveniente adoptar una noción operativa y funcional de inteligencia artificial, entendida, de forma general, como un conjunto de algoritmos orientados a que los sistemas o máquinas emulen funciones propias de la inteligencia humana, capaces además de perfeccionarse mediante la retroalimentación constante a partir de la información que recaban[13]. En palabras de Goretty Carolina Martínez, "un sistema inteligente es aquél que exhibe un comportamiento similar al humano cuando se enfrenta a un problema idéntico y no seamos capaces de distinguir entre un ser humano y un programa de computadora en una conversación a ciegas"[14].

Por su parte, el *machine learning* —o aprendizaje automático— ha sido descrito por Alpaydin como un proceso que permite a los sistemas optimizar su desempeño mediante la exposición repetida a ejemplos previos y datos históricos, sin necesidad de ser programados explícitamente para cada tarea específica[15].

En el ámbito tributario internacional, diversas administraciones fiscales han adoptado herramientas basadas en IA con el fin de mejorar su capacidad para combatir la evasión fiscal y el fraude, establecer modelos de clasificación de riesgos (que incluyen desde la omisión en el entero de contribuciones hasta el lavado de dinero o la emisión de Comprobantes Fiscales Digitales por Internet [CFDI] sin sustancia económica), así como para brindar asistencia al contribuyente. En este contexto, se han desarrollado programas informáticos que, apoyados en IA, permiten agrupar a los contribuyentes con base en atributos previamente definidos, detectar transacciones atípicas conforme a patrones de comportamiento tributario y ofrecer herramientas de asistencia virtual en el cumplimiento de las obligaciones fiscales[16].

Para que estas soluciones tecnológicas operen con eficacia, resulta indispensable un proceso integral de digitalización del sector público. Esta digitalización no se restringe al ámbito fiscal, sino que ha permeado transversalmente a otras áreas administrativas del Estado, lo cual ha permitido incorporar tecnologías digitales en sus procesos internos y en sus canales de interacción con los particulares, con el objetivo declarado de aumentar la eficiencia y efectividad de su gestión.

[13] *Cfr. https://www.oracle.com/mx/artificial-intelligence/what-is-ai/*, visitada el 6 enero de 2025.

[14] Martínez Bahena, Goretty Carolina, "La Inteligencia Artificial y su Aplicación al Campo del Derecho", en *Alegatos*, Septiembre/diciembre 2012, p. 828.

[15] "*Machine learning is programming computers to optimize a performance criterion using example data or past experience*." En Alpaydin, Ethem. *Introduction to Machine Learning*. 2a ed. Cambridge, MA: MIT Press, 2010.

[16] *Cfr*. Ossandón Cerda, Francisco, "Inteligencia Artificial en las Administraciones Tributarias: Oportunidades y Desafíos", en *Revista de Estudios Tributarios*, 2020, p. 124.

En retrospectiva, el desarrollo de la relación fisco-contribuyente ha experimentado una transformación radical. Queda ya lejano aquel periodo en que los contribuyentes adherían etiquetas con códigos de barras[17] a sus facturas impresas, o cuando, en los últimos años del siglo XX, los contadores públicos debían cargar en los sistemas del SAT los dictámenes fiscales a través de plataformas rudimentarias que colapsaban por la saturación en fechas clave[18]. Esta evolución, que parecía inconcebible en la época en que se temía que la infraestructura digital colapsaría con el llamado *Y2K*[19], ha dado lugar a una realidad insoslayable: hoy, la Fiscalía de Argentina utiliza el software *Prometea*[20], capaz de elaborar dictámenes jurídicos aplicando IA, reduciendo en un 99% el tiempo necesario respecto de los métodos tradicionales.

En este entorno, ha surgido un debate relevante: ¿puede un sistema dotado de IA —sin intervención humana directa— tener competencia y facultades para practicar una revisión electrónica o incluso imponer sanciones[21]. Esta cuestión, de enorme trascendencia jurídica, pone en tensión los principios fundamentales del derecho administrativo sancionador, particularmente los de legalidad y debido proceso.

En el caso mexicano, el SAT ha incorporado aplicaciones concretas de *machine learning*[22] para analizar grandes volúmenes de datos derivados, principalmente, de la emisión masiva de CFDI. Mediante el uso de algoritmos matemáticos, se agrupan y clasifican los datos de facturación con el fin de identificar patrones de comportamiento que permitan detectar prácticas simuladas, como la emisión de comprobantes fiscales sin sustancia económica. Dichos patrones son utilizados para establecer reglas que, al ejecutarse, generan alertas o hipótesis de riesgo fiscal, particularmente en relación con la materialidad de las operaciones facturadas.

Asimismo, esta tecnología le permite al SAT realizar análisis de riesgo orientados a la detección de posibles omisiones en el entero de contribuciones, considerando características particulares de los diversos sectores económicos que integran la base tributaria. Para dotar de respaldo normativo a estas prácticas, se reformó el Artículo 33, fracción I, inciso

---

[17] Aunque no nos referimos al Código de Barras Dimensional, ni Código QR, *https://www.sat.gob.mx/consulta/80521/requisitos-de-los-comprobantes-en-papel,* visitada el 5 diciembre de 2024.

[18] Conocido como el SIPRED96. Sin embargo, este empieza a utilizarse en el año de 1997.

[19] *https://www.britannica.com/technology/Y2K-bug*, visitada el 19 de enero de 2025.

[20] Ossandón Cerda, Francisco, *op. cit*., p. 124.

[21] *Cfr*. *https://institutoitf.cl/un-robot-te-multo-nuevas-tecnologias-en-administraciones-fiscales/*.

[22] O Aprendizaje Automático es una rama de la IA que, mediante algoritmos, dota a los ordenadores de la capacidad de identificar patrones en datos masivos (*Big data*) y elaborar predicciones (análisis predictivo). *Cfr. https://www.iberdrola.com/innovacion/machine-learning-aprendizaje-automatico*, visitada el 20 enero de 2025.

i) del Código Fiscal de la Federación (CFF)[23], incorporando expresamente la posibilidad de que la autoridad fiscal difunda a los contribuyentes del Impuesto sobre la Renta (ISR) los denominados "parámetros de referencia". Estos parámetros incluyen datos relativos a utilidades, conceptos deducibles o tasas efectivas de impuesto observadas en otras entidades o figuras jurídicas que operan en el mismo sector económico.

Gracias a estos elementos, el SAT se encuentra en condiciones de realizar mediciones de riesgo fiscal y, de manera preventiva, emitir comunicaciones a los contribuyentes —comúnmente denominadas "cartas invitación"— cuando detecta que se apartan significativamente de los parámetros de referencia. Cabe destacar que tales comunicaciones no constituyen el inicio formal del ejercicio de facultades de comprobación, ya que se enmarcan en los denominados programas de cumplimiento voluntario.

Todo lo anterior nos inserta de lleno en un nuevo paradigma que Javier Echeverría ha conceptualizado como el "tercer entorno", en el cual se desarrolla actualmente la actividad humana. Según este autor:

> El primero es el de la naturaleza, en el que transcurre la sociedad rural agraria basada en el trabajo del campo (*physis*), donde los tiempos son los de las estaciones y, por ende, se trata de tiempos largos; el segundo es el entorno de la ciudad (*polis*), de la industria y del mercado, donde los tiempos ya se aceleran y se fabrica en masa; y el tercer entorno es el electrónico, el espacio de la sociedad de la información, que se superpone a los dos anteriores y coexiste con ellos. Aquí el poder económico lo tienen quienes manejan la conectividad y las redes[24].

En este tercer entorno, los elementos estructurales de la interacción social se modifican sustancialmente. La distancia geográfica pierde relevancia, las redes digitales se convierten en los nuevos espacios de confluencia, y quienes no son nativos digitales[25] deben adaptarse aceleradamente a esta nueva realidad. Aunque esta transformación venía gestándose desde los albores del siglo XXI, fue durante la pandemia por COVID-19[26] que su adopción se intensificó de manera exponencial, evidenciando su carácter irreversible.

Este nuevo marco sociotecnológico plantea desafíos mayúsculos al Estado de Derecho, particularmente en lo que respecta a la garantía de seguridad jurídica en el ámbito

[23] DOF del 8 de diciembre de 2020, *https://dof.gob.mx/nota_detalle.php?codigo=5606951&fecha=08/12/2020#gsc.tab=0*, visitada el 18 enero de 2025.

[24] Citado por Luz Clara, B. B., "Tecnología, derecho y conflictos", en *Revista Mexicana de Ciencias Penales 3*(10), 2020, pp. 35-46, recuperado a partir de *https://revistaciencias.inacipe.gob.mx/index.php/02/article/view/96*, visitado el 13 de febrero de 2025.

[25] *Idem*. Término acuñado y divulgado por Marck Prensky en su libro Inmigrantes digitales (2001) para indicar a los niños nacidos desde 1990 en adelante, para quienes utilizar los elementos tecnológicos es muy sencillo, a diferencia del resto de las personas que tienen que aprender y esforzarse.

[26] Ocasionada por el virus SARS-COV-2.

fiscal. La utilización intensiva de tecnologías de IA y el empleo masivo de datos personales —algunos sensibles— obliga a repensar los límites normativos de la potestad tributaria, así como a examinar con rigor los mecanismos de control, transparencia y rendición de cuentas que deben imperar en el uso de estas herramientas digitales por parte de las autoridades fiscales.

III. NOTAS SOBRE LA SEGURIDAD JURÍDICA EN MATERIA TRIBUTARIA

La seguridad jurídica, desde una perspectiva etimológica y normativa, es definida por la Real Academia Española como la *cualidad del ordenamiento jurídico que implica la certeza de sus normas y, consiguientemente, la previsibilidad de su aplicación*. En diversos países, como en España, esta figura constituye un principio de rango constitucional[27].

En el ámbito del Derecho mexicano, este principio se encuentra cimentado en la propia Constitución, particularmente cuando establece que todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que el propio texto constitucional establece[28].

La fuerza normativa de este precepto es evidente: la Constitución se erige como norma suprema del orden jurídico, por lo que cualquier disposición de legislación secundaria que limite, restrinja o suspenda derechos humanos, fuera de los casos constitucionalmente autorizados, constituye una violación a estos derechos. Esta preeminencia del orden constitucional ha sido reiteradamente reconocida por el Poder Judicial de la Federación en diversos criterios jurisprudenciales[29].

El jurista Elías Díaz ha señalado que:

> El Estado de Derecho es aquel en el que el poder y la actividad estatal se encuentran regulados y controlados por el Derecho. Las ideas de control jurídico, de regulación legal de la actividad estatal y de la limitación del poder mediante el sometimiento a la ley, aparecen como esenciales al concepto de Estado de Derecho, en constante relación con el respeto a la persona humana y sus derechos fundamentales[30].

Sin embargo, tales principios solo adquieren eficacia cuando están dotados de fuerza normativa real. La sola consagración formal de principios como la irretroactividad de la ley, la publicación obligatoria de las normas o el sometimiento de la administración a la legalidad carecería de sentido si las leyes fueran oscuras o imprecisas, o si los jueces pudieran

[27] Voz "seguridad jurídica" en la versión electrónica de la Real Academia Española, visible en *http://dle.rae.es/?id=X-TrIaQd*, visitada el 20 de diciembre de 2024.

[28] Artículo 1o. Constitución Política de los Estados Unidos Mexicanos.

[29] Entre otras, la de rubro: "CONSTITUCIÓN. SUPREMACÍA DE LA.", Segunda Sala, Quinta Época, *Semanario Judicial de la Federación*, t. LXXIII, p. 7848, Registro Digital: 326474.

[30] Díaz, Elías, *Estado de Derecho y Sociedad Democrática*, Madrid, Taurus, pp.17-18.

actuar conforme a sus convicciones personales y no al Derecho. La seguridad jurídica requiere, por tanto, no solo la existencia de tales principios, sino su plena aplicación y tutela efectiva.

En materia tributaria, la relación jurídica se manifiesta como un vínculo de derechos y obligaciones entre el Estado y los particulares. La obligación de contribuir al gasto público no solo recae sobre los gobernados, sino también impone límites al actuar del Estado, que debe someterse a normas legales claras que permitan a los contribuyentes conocer con certeza el objeto, la base, la tarifa, el momento y la forma en que deben cumplirse las contribuciones, así como garantizar que la actuación de las autoridades se realice exclusivamente por funcionarios competentes y expresamente facultados por ley.

Pérez de Ayala y González García, al referirse al principio de legalidad tributaria, señalan que:

> En su concepción más estricta, este principio exige que los sacrificios patrimoniales solo puedan imponerse mediante ley, entendida como la expresión de una voluntad soberana legítimamente constituida, manifestada en la forma solemne establecida y con fuerza obligatoria. Solo así se habilita también la revisión judicial correspondiente[31].

Estos autores identifican este principio con el de reserva de ley, cuyo propósito es limitar la potestad normativa del Estado al imperio exclusivo de la ley. Así, la reserva puede ser[32]:

- Absoluta o estricta, cuando toda la materia debe ser regulada exclusivamente por ley formal o actos con fuerza de ley;
- Relativa o atenuada, cuando la ley debe establecer al menos los elementos esenciales del tributo, permitiendo al Ejecutivo desarrollar aspectos secundarios.

Este último modelo es el que caracteriza al sistema tributario mexicano. La Constitución impone al legislador la obligación de determinar los elementos esenciales de los tributos, y cualquier exceso del Ejecutivo al pretender definirlos a través de reglamentos o reglas generales vulnera el principio de legalidad, atentando contra la seguridad jurídica del contribuyente.

En esta línea, Arrioja Vizcaíno sostiene que:

> La autoridad hacendaria no puede realizar ningún acto ni ejercer ninguna función en el ámbito fiscal sin estar previa y expresamente facultada por una ley aplicable al caso. Del mismo modo, los contribuyentes solo están obligados a cumplir con

[31] Pérez de Ayala, José Luis y González García, Eusebio. *Derecho Tributario*, Salamanca, Plaza Universitaria, t. I, pp. 33-34.
[32] *Cfr*. *Ibid.*, p. 146.

las disposiciones que les impongan deberes de manera clara, expresa y legalmente establecida[33].

Aunado a ello, este principio no solo exige al gobernado conocer sus obligaciones frente al fisco, sino también identificar con claridad los derechos que puede ejercer frente al Estado cuando este pretenda actuar más allá del marco legal que regula su actuación recaudatoria.

Delgadillo Gutiérrez, retomando la doctrina de Adam Smith, reafirma la vigencia del principio de certidumbre al destacar que toda norma tributaria debe especificar con claridad: el sujeto, el objeto, la cuota, el método de valuación, la forma de pago, los plazos, las sanciones aplicables, etc., lo que impone la exigencia de que las leyes fiscales sean comprensibles, precisas y accesibles[34].

Este principio, consagrado en el Artículo 31, fracción IV de la Constitución, obliga al Estado no solo a legislar con justicia en materia tributaria, sino también a garantizar al contribuyente un conocimiento claro y anticipado de su situación fiscal. La Suprema Corte de Justicia de la Nación ha interpretado este principio en el sentido de que solo el legislador puede establecer los elementos esenciales de los tributos[35], con un grado razonable de claridad y precisión, que permita a los gobernados anticipar las consecuencias jurídicas y económicas de sus actos.

Por ello, el principio de legalidad en materia tributaria constituye uno de los pilares de la seguridad jurídica del gobernado. Su observancia permite al contribuyente prever las consecuencias jurídicas derivadas de su actuación y anticipar el impacto económico de sus decisiones fiscales.

La relevancia de este principio se acentúa en el contexto actual, en el que la determinación y revisión de las obligaciones fiscales se realiza, en muchos casos, por medios electrónicos, como las revisiones electrónicas o la presentación de declaraciones a través de plataformas digitales. Este fenómeno será analizado en el siguiente apartado.

IV. ESCENARIOS DE RIESGO PARA LA ESTABILIDAD NORMATIVA

Si bien resulta indiscutible que la inteligencia artificial (IA) ha aportado beneficios significativos en diversos ámbitos de nuestra vida cotidiana, el procesamiento masivo de datos que implica su utilización para optimizar resultados y ejecutar programas orientados al cumplimiento y verificación de las obligaciones tributarias, conforme al marco constitucional

[33] Arrioja Vizcaíno, Adolfo, *Derecho Fiscal*, 2a. ed., México, Themis, p. 18.
[34] Delgadillo Gutiérrez, Luis Humberto, *Principios de Derecho Tributario*, 3a. ed., México, Limusa, p. 39.
[35] P./J. 106/2006, *Semanario Judicial de la Federación y su Gaceta*, t. XXIV, Octubre de 2006, p. 5, Registro Digital: 174070.

mexicano, plantea serias tensiones con el principio de seguridad jurídica en materia fiscal. En este escenario, ya no se discute simplemente la validez de obligaciones como la de llevar contabilidad electrónica con determinadas características, ni la legitimidad de compartir dicha información con la autoridad fiscal en ausencia de una notificación formal del inicio de facultades de comprobación.

Ejemplo paradigmático de la complejidad actual es el fenómeno de las operaciones simuladas, que ha evolucionado desde la utilización de facturas apócrifas hasta la emisión de Comprobantes Fiscales Digitales por Internet (CFDI) válidos en forma, pero que encubren transacciones inexistentes. Este problema ha sido objeto de estudio por un grupo multidisciplinario de investigadores del Centro de Ciencias de la Complejidad (C3) y el Instituto de Física de la UNAM, en colaboración con el *Department of Network and Data Science de la Central European University*, en Hungría, quienes mediante IA detectaron que esta práctica evasiva creció de 40 mil millones de pesos en 2015 a 77 mil millones en 2018, lo que representa un alarmante incremento del 93%[36], tendencia que lamentablemente se mantiene al alza y no es exclusiva de México.

Aunado a lo anterior, se ha intensificado sustancialmente la práctica de revisiones electrónicas[37] por parte de la autoridad fiscal, sin que el gobernado tenga certeza sobre la legitimidad del funcionario responsable o incluso si dicha revisión ha sido realizada por un algoritmo de IA. La opacidad respecto a la duración, el alcance o la identidad del ente fiscalizador es tal, que el contribuyente puede encontrarse bajo vigilancia constante sin saberlo, siendo notificado sólo hasta la emisión de una resolución provisional, sin información sobre el cómo, quién, cuándo o sobre qué ejercicios se efectuó dicha fiscalización.

Aunque las tradicionales visitas domiciliarias o de gabinete[38] no han desaparecido por completo, su uso se ha vuelto cada vez más esporádico. Las nuevas tecnologías permiten a la autoridad analizar de forma automatizada los datos que los contribuyentes proporcionan en tiempo real, ya sea al emitir o recibir un CFDI o al enviar mediante el buzón tributario su contabilidad electrónica, lo que incluye el catálogo de cuentas, la balanza de comprobación mensual y, en su caso, información de pólizas y auxiliares.

En este contexto, el ejercicio de las facultades de comprobación por parte de la autoridad fiscal ha experimentado una transformación sustancial. El análisis de docu-

[36] Vargas-Parada, Laura, "Inteligencia artificial y ciencia de redes contra la evasión fiscal", Recuperado de *https://www.c3.unam.mx/pdf/noticias/NOTICIA_174.pdf*, visitado el 20 diciembre 2024.

[37] Art. 42 Fr. IX y 53-B del Código Fiscal de la Federación.

[38] Art. 42 Fr. II y III del Código Fiscal de la Federación.

mentos físicos ha sido desplazado por la utilización de sistemas informáticos dotados de IA, conocidos como "sistemas expertos", los cuales, en palabras de Julio Téllez, comprenden:

a) Una base de conocimientos estructurada que permite realizar cálculos lógicos;
b) Un sistema cognoscitivo que incorpora mecanismos de inferencia con esquemas de razonamiento propios del dominio;
c) Una interfaz que permite la comunicación entre el usuario y la máquina"[39].

Es en este punto donde se abren espacios de vulnerabilidad a los delitos informáticos, los cuales representan serias amenazas a la seguridad jurídica en el ámbito tributario. Por ello, se torna imperativo replantear la protección de los datos personales en este contexto. Aunque la materia está regulada en términos generales, consideramos que requiere una adecuación específica al ámbito fiscal, dado que su regulación aún es incipiente y puede derivar en transgresiones anticipadas a derechos fundamentales.

A diferencia de la perspectiva que sostiene Gabriela Ríos Granados, quien señala que la afectación a la seguridad jurídica en esta materia se origina en la falta de legalidad formal, al estar muchas de las normas contenidas en reglas de carácter general en lugar de leyes expedidas por el Congreso, aquí sostenemos que el problema principal radica en el tratamiento y protección de los datos personales proporcionados a la autoridad fiscal para el cumplimiento de obligaciones tributarias[40].

Desde un enfoque internacional, el Pacto Internacional de Derechos Civiles y Políticos, aprobado en 1966 y en vigor desde 1976, constituye el primer instrumento multilateral que consagra la protección de la privacidad. Su Artículo 17 establece que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación"[41]. Esta protección ha sido perfeccionada por el Comentario General Núm. 16, el cual establece que la recolección y almacenamiento de información personal en computadoras y bases de datos debe estar regulada por ley; que el Estado debe garantizar que dicha información no sea accedida por personas no autorizadas; y que los individuos deben tener derecho a conocer, corregir o eliminar información sobre ellos.

---

[39] Téllez Valdez, Julio, *op. cit*., p. 48.

[40] *Cfr*. Ríos Granados, Gabriela, "Innovación tecnológica en la gestión tributaria. Un estudio comparado: España y México", *Bol. Mex. Der. Comp.,* V. dic. 2003. 36. N. 108, p. 11, disponible en *https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3775*, visitado el 15 enero de 2025.

[41] *https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights*, visitada el 15 de enero de 2025.

En el caso mexicano, la protección de los datos personales en poder del fisco encuentra fundamento en el Artículo 6o., fracción II[42], apartado A), y en el segundo párrafo[43] del Artículo 16 de la Constitución, y se desarrolla en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[44]. Si bien existe también la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[45], ésta aplica exclusivamente al sector privado, mientras que la primera es la aplicable a autoridades de todos los niveles de gobierno.

La citada Ley General tiene como objeto establecer bases mínimas y condiciones homogéneas para el tratamiento de datos personales y garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO[46]), así como la observancia de los principios de protección de datos. En cuanto a los datos sensibles[47], la regla general es que no podrán tratarse sin el consentimiento expreso del titular, salvo en los supuestos del Artículo 16, fracción V, que permite su tratamiento cuando sea necesario para ejercer un derecho o cumplir con una obligación derivada de una relación jurídica.

Esto implica que el SAT y otras autoridades fiscales no requieren consentimiento expreso para el tratamiento de estos datos, dada la relación jurídica derivada de las obligaciones tributarias. No obstante, la ley en cuestión carece de disposiciones efectivas para garantizar la seguridad de los datos en posesión de los sujetos obligados, así como de un catálogo robusto de infracciones y sanciones. En palabras de Nuhad Ponce Kuri, "toda norma jurídica es una regla imperativa de conducta, cuya violación genera la consecuencia de una posible imposición de sanción por parte del órgano del Estado que sea competente para ello..."[48].

---

[42] La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Para tal efecto, los sujetos obligados contarán con las facultades suficientes para su atención.
Por lo que hace a la información relacionada con los datos personales en posesión de particulares, la ley a la que se refiere el Artículo 90 de esta Constitución determinará la competencia para conocer de los procedimientos relativos a su protección, verificación e imposición de sanciones.

[43] Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

[44] *https://www.dof.gob.mx/nota_detalle.php?codigo=5752569&fecha=20/03/2025#gsc.tab=0,* visitada el 10 de abril de 2025.

[45] *https://www.dof.gob.mx/nota_detalle.php?codigo=5752569&fecha=20/03/2025#gsc.tab=0,* visitada el 10 de abril de 2025.

[46] Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información

[47] Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para ésta. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

[48] Ponce Kuri, Nuhad, "Del Procedimiento de Imposición de Sanciones", en Tenorio Cueto, Guillermo A. (coord.), *Ley Federal de Protección de Datos Personales en Posesión de los Particulares Comentada*, México, INAI, 2019, p. 207.

A diferencia de lo anterior, la ley aplicable a los particulares contempla en su Artículo 59 un régimen sancionador amplio, con multas que oscilan entre 100 a 320,000 veces la Unidad de Medida y Actualización por conductas como incumplir con la confidencialidad, vulnerar la seguridad de bases de datos, transferir información sin consentimiento o con fines ilegítimos, entre otros. Dichas sanciones pueden duplicarse en caso de reincidencia o si se trata de datos sensibles. Además, el Artículo 62 prevé responsabilidad civil, penal y penas de prisión en ciertos casos.

En materia penal, el Código Penal Federal regula en su Título Noveno, Capítulo II, las conductas relacionadas con el acceso ilícito a sistemas y equipos informáticos. Los Artículos 211 bis 1 a 211 bis 5 prevén sanciones que van de tres meses a diez años de prisión, dependiendo del tipo de intrusión, del daño causado y de si el autor tenía o no autorización para acceder al sistema afectado. Sin embargo, dichas disposiciones resultan insuficientes ante la sofisticación actual del cibercrimen y la deficiente técnica legislativa. Como advierte Cinthya Solís: "el juez no entiende cómo se lleva a cabo la conducta y le es muy difícil encuadrar el delito informático en un tipo penal existente... Si te falta un elemento, no hay delito que perseguir y dejan libres a los ciberatacantes"[49].

En síntesis, la clásica concepción de seguridad jurídica en el ámbito fiscal se ve rebasada por riesgos ajenos tanto a la autoridad como al contribuyente. La vulneración, modificación o eliminación de datos mediante delitos informáticos representa un riesgo permanente, perpetrado desde cualquier parte del mundo.

En este sentido, varios países han adherido al Convenio sobre la Ciberdelincuencia del Consejo de Europa[50] (Convenio de Budapest), principal instrumento internacional en la materia. Este convenio tipifica conductas como el acceso deliberado e ilegítimo a sistemas informáticos, la interceptación de datos, el daño o eliminación de información, la falsificación informática y el fraude cometido mediante interferencia en sistemas informáticos, acceso deliberado e ilegítimo a todo o parte de un sistema informático; interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo; cualquier acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos; introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos; actos deliberados e

[49] *https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/*, visitada el 20 enero de 2025.

[50] Aunque también lo han ratificado Japón, Estados Unidos, Chile, Argentina, Australia, Israel entre otros. México es simple observador.

ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra entre otros, todos ellos relevantes para garantizar la seguridad jurídica en el nuevo entorno digital fiscal[51].

México aún no es signatario del Convenio citado, por lo que se evidencia poca voluntad de sancionar penalmente las infracciones cometidas, y menor de legislar, o de estructurar políticas públicas efectivas para evitar la intromisión de los ciberdelincuentes a los sistemas informáticos del SAT o de los contribuyentes, que traigan como consecuencia con la modificación o supresión de datos que implique el que éstos se encuentren en falta en el cumplimiento de sus obligaciones fiscales.

Nos referimos entre otros, a hechos como modificación de elementos que conforman la base gravable de los tributos. Así al incrementarse artificialmente los ingresos de un contribuyente o reducirse sus pérdidas o deducciones, podrán situarlo en una situación de haber cubierto una cantidad menor del débito fiscal.

Igualmente se podrían alterar los avisos presentados, o inclusive eliminarlos del sistema del SAT, con lo cual es evidente la infracción hipotéticamente cometida, así como sus consecuencias fiscales.

Imaginemos también un caso de *ramsonware*[52] por el que se inhabilita el uso de los datos contenidos en el equipo de cómputo de un contribuyente durante el ejercicio de facultades de comprobación o cerca de la temporada de cumplimiento de alguna obligación tributaria.

También podríamos hablar de casos sobre robo de identidad[53] a través de la cual un tercero haciéndose pasar por un contribuyente, autentica con la firma electrónica de aquél, diversa documentación que traerá perjuicios al referido contribuyente, desde omisión de ingresos, suscripción de garantías, emisión de diferentes tipos de CFDI, etc.

Si bien como concepto el robo de identidad pudiera suponer al lector que solamente se realiza mediante muy sofisticados equipos, o que se encuentra dirigido contra per-

---

[51] *Cfr.https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf*, visitada el 20 de enero de 2025.

[52] Software malicioso que cifra los datos de un equipo para exigir dinero. Si el usuario no le paga al cibercriminal en un cierto plazo, no puede recuperar los datos y los pierde para siempre. Visible en *https://mx.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html*, visitada el 20 de enero de 2025.

[53] El robo o suplantación de identidad es el delito informático de más rápido crecimiento en el mundo. Conocido también como *impersonation*, se entiende como suplantación de personalidad o identidad a quien funge ser una persona que no es. El caso más común es el robo o la utilización de tarjetas de crédito y documentos de terceros. Visible en *https://iusnava.com/2020/05/17/usurpacion-de-identidad/*, visitada el 20 de enero de 2025.

sonajes públicos de gran notoriedad, lo cierto es que no, puesto que se realiza de manera masiva, mediante las siguientes acciones, que detalla Raúl Cervantes[54]:

> *Phishing* (solicitar información mediante correos falsos). Es la duplicación de una página web para que el visitante crea que se encuentra en el portal original en lugar de uno duplicado.
> *Tabjacking*. Este tipo de ataque es conocido con este término y básicamente consiste en una página que, luego de un tiempo de inactividad, es reemplazada por otra que puede verse como la original, por eso es tan peligroso como cualquier otro *phishing*.
> *Pharming* (robo de información mediante el uso de páginas falsas). Es una nueva modalidad de fraude *on line* que consiste en suplantar el sistema de resolución de nombres de dominio (*Domain Name Server* o DNS) para conducir al usuario a una página web falsa. Aunque es una amenaza creciente y peligrosa, la solución está en la prevención y en un antivirus eficaz.

Cuando un usuario teclea una dirección en su navegador, esta debe ser convertida a una dirección de protocolo de Internet numérica (IP). Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores DNS, en los que se almacenan tablas con las direcciones IP de cada nombre de dominio.

Spam y spyware (archivos malignos dentro de correos electrónicos). El spam son mensajes no solicitados y enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es por correo electrónico. Otras tecnologías de Internet que han sido objeto de *spam* incluyen grupos de noticias, motores de búsqueda y blogs. El *spam* puede tener también como objetivo los celulares y los sistemas de mensajería instantánea.

Por su parte, el *spyware* es un *software* que recopila información de una computadora y después la transmite a una entidad externa sin el conocimiento o el consentimiento del propietario. Un *spyware* típico se autoinstala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha la computadora (utiliza el CPU y la memoria RAM, reduciendo así la estabilidad) y funciona controlando todo el tiempo el uso que se hace de Internet y mostrando anuncios relacionados.

Es probable que el lector llegue a pensar que los ejemplos descritos líneas arriba, son mera especulación hipotética de quien esto escribe. Sin embargo, la realidad es que los ciberataques son mucho más comunes de lo que nos imaginamos y el pensar que el SAT en México o la Agencia de cualquier lugar del mundo que se dedique al cobro y administración de tributos son inmunes a este tipo de ataques por ser órgano o agencias del

[54] *Idem*.

gobierno, es totalmente ilusorio, como a continuación y a guisa de ejemplo se comentarán algunos ejemplos:

En 2020, presumiblemente el grupo Lazarus utilizó el *framework* de ciberespionaje MATA para atacar múltiples sistemas operativos, incluyendo Windows, macOS y Linux. Este *malware* permitió a los atacantes robar bases de datos, distribuir *ransomware* e instalar puertas traseras en sistemas infectados, afectando redes corporativas y sistemas financieros[55].

Más tarde en 2022 el grupo de *ransomware* Conti comprometió los servidores del Ministerio de Hacienda de Costa Rica, afectando la plataforma de Administración Tributaria Virtual (ATV) utilizada para la presentación de declaraciones de impuestos por parte de ciudadanos y empresas. Los atacantes afirmaron haber robado 1 terabyte de información y exigieron un rescate de 10 millones de dólares[56].

A finales del año pasado, para efectos de México, la oficina de asuntos legales de la Presidencia de la República sufrió un ataque de *ransomware*. Los atacantes publicaron muestras de información personal de empleados gubernamentales y amenazaron con divulgar 313 gigabytes de archivos si no se cumplían sus demandas en un plazo de 10 días. El Presidente Andrés Manuel López Obrador confirmó que el gobierno estaba investigando el incidente, sin que se haya conocido con detalle la información sustraída[57].

Inclusive, el propio SAT en México ha reconocido la existencia de miles de correos electrónicos apócrifos, que aparentan proceder de dicha institución y ha alertado a los contribuyentes mexicanos mediante el diseño y puesta en operación de una aplicación para que los mismos puedan identificar cientos de correos apócrifos[58] creados con la intención del robo de datos fiscales, detallando que si luego de efectuar la búsqueda en el mismo: "Si aparece "Registrado como correo apócrifo", ¡no descargues ningún archivo!", con lo que expresamente está reconociendo el grave riesgo que gravita sobre los datos de particulares al cumplir con sus obligaciones fiscales mediante plataformas electrónicas.

No obstante, es suficiente la narrativa anterior para poner a debate el riesgo que implica para la seguridad jurídica de los contribuyentes la falta de políticas públicas efectivas que tiendan a robustecer los sistemas informáticos de la autoridad donde se alojan miles de datos sensibles de los gobernados, y el resarcimiento de los daños que se les puede causar por un ciberataque.

[55] *https://es.wikipedia.org/wiki/Kaspersky_Lab?utm_source=chatgpt.com*, visitada el 18 de enero de 2025.

[56] *https://en.wikipedia.org/wiki/2022_Costa_Rican_ransomware_attack?utm_source=chatgpt.com*, visitadas el 18 de enero de 2025.

[57] *https://apnews.com/article/mexico-president-hacking-attack-ransomhub-ransomware-a97fa044850ba05f574f-71d2af3d67c8*, visitada el 19 de enero de 2025.

[58] *http://omawww.sat.gob.mx/gobmx/Paginas/buscadorcorreosapocrifos/buscador.html*, visitada el 21 de enero de 2025.

V. CONCLUSIONES

La seguridad jurídica, entendida como una condición esencial del Estado de Derecho, exige que los contribuyentes puedan formar expectativas razonables y fundadas respecto de la actuación de la autoridad fiscal. Esta expectativa descansa en la premisa de que dicha autoridad se encuentra constreñida a actuar dentro del marco legal y conforme a las facultades expresamente conferidas por la legislación tributaria.

Dentro del sistema fiscal mexicano, la determinación del monto de las contribuciones a cargo de los particulares obedece a un modelo autodeclarativo. En él, el sujeto obligado calcula su carga tributaria deduciendo de sus ingresos acumulables las pérdidas fiscales y demás deducciones autorizadas por la normativa vigente. A pesar de que la autodeterminación representa un ejercicio de confianza legislativa en el cumplimiento espontáneo de los contribuyentes, la autoridad fiscal conserva la facultad de verificar la veracidad de las declaraciones mediante los procedimientos establecidos en el orden jurídico.

Tradicionalmente, esta relación jurídico-tributaria se estructuraba de forma binaria entre el contribuyente y el fisco. No obstante, la irrupción de tecnologías avanzadas en el ámbito tributario, especialmente aquellas asociadas al uso de medios electrónicos, plataformas digitales y herramientas de inteligencia artificial, ha transformado de manera sustantiva los modos de cumplimiento fiscal. Se ha transitado, en efecto, de registros manuales a sistemas de contabilidad electrónica; de declaraciones impresas presentadas físicamente —cuyo pago solía efectuarse mediante cheque en ventanilla bancaria— a esquemas automatizados de declaración prellenada, en los que intervienen asistentes virtuales y cuya liquidación se realiza por medio de transferencias electrónicas en plataformas bancarias digitales.

Este proceso de digitalización ha favorecido el intercambio automatizado de datos entre los contribuyentes y la autoridad hacendaria, elevando así la eficiencia de la administración tributaria. Sin embargo, esta transformación tecnológica no ha estado exenta de riesgos. El flujo masivo de información fiscal, en buena medida gestionado por sistemas informáticos y algoritmos, ha propiciado la intervención de terceros ajenos a la relación jurídica principal. Tales terceros, en algunos casos, pueden manipular datos sensibles sin el consentimiento de las partes involucradas, generando afectaciones tanto para los particulares como para la propia administración fiscal.

En este contexto, se impone como una necesidad inaplazable la actualización del marco normativo, con el propósito de adecuarlo a las condiciones de una fiscalidad digitalizada y garantizar, al mismo tiempo, la plena tutela de los derechos de los contribuyentes y la seguridad jurídica de los actos administrativos. Esta actualización legislativa debe

contemplar, entre otros aspectos, la instauración de mecanismos jurídicos que aseguren la integridad, autenticidad y confidencialidad de los datos fiscales, así como el establecimiento de procedimientos eficaces para la reparación de los daños que puedan derivarse de vulneraciones tecnológicas. La normatividad actualmente vigente ha sido, en muchos aspectos, superada por la acelerada evolución tecnológica, lo que obliga al legislador a prever soluciones jurídicas que armonicen innovación con legalidad y control institucional.

VI. FUENTES DE INFORMACIÓN

1. *Bibliografía*

ARRIOJA VIZCAÍNO, Adolfo, *Derecho Fiscal*, 2a. ed., México, Themis, 1985.

DELGADILLO GUTIÉRREZ, Luis Humberto, *Principios de Derecho Tributario*, 3a. ed., México, Limusa, 1987.

DÍAZ, Elías, *Estado de Derecho y Sociedad Democrática*. 1a. ed., México, Taurus, 1971.

PÉREZ DE AYALA, José Luis y GONZÁLEZ GARCÍA, Eusebio, *Derecho Tributario*. 1a. ed., Salamanca, Plaza Universitaria, t. I, 1994.

PONCE KURI, Nuhad, "Del Procedimiento de Imposición de Sanciones", en TENORIO CUETO, Guillermo A. (coord.), *Ley Federal de Protección de Datos Personales en Posesión de los Particulares Comentada*", 1a. ed., México, INAI, 2019.

TÉLLEZ VALDEZ, Julio, *Derecho Informático*. 2a. ed., México, Mc Graw Hill, 1998.

2. *Legislación*

Código Fiscal de la Federación.

Constitución Política de los Estados Unidos Mexicanos.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

3. *Páginas electrónicas*

http://dle.rae.es/?id=XTrIaQd.

http://omawww.sat.gob.mx/tramitesyservicios/Paginas/documentos/guiaanexo20_07092017.pdf.

https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_conferencias_varsovia_2013_resol_proteccion_datos.pdfhttp://dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017.

http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010.

*https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_*

Budapest_y_Ciberdelincuencia_en_Chile.pdf.
https://mx.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html
https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/.
http://www5.diputados.gob.mx/index.php/camara/Centros-de-Estudio/CESOP/Estudios-e-Investigaciones/Revista-Legislativa-CESOP.
https://revistaciencias.inacipe.gob.mx/index.php/02/article/view/96.
https://www.eleconomista.com.mx/tecnologia/Ataque-a-Loteria-Nacional-seria-el-segundo-caso-de-ransomware-en-el-gobierno-de-AMLO-20210531-0090.html.
https://www.ionos.mx/digitalguide/paginas-web/desarrollo-web/que-es-un-gigabyte/.
https://expansion.mx/opinion/2020/06/12/mexico-lejos-de-los-derechos-digitales.
http://cedhj.org.mx/revista%20DF%20Debate/revista%20pdf/ADEBATE%2012-2020.pdf.
https://www.corteidh.or.cr/tablas/r33897.pdf.
https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx.
https://www.oracle.com/mx/artificial-intelligence/what-is-ai/.
https://www.britannica.com/technology/Y2K-bug.
https://institutoitf.cl/un-robot-te-multo-nuevas-tecnologias-en-administraciones-fiscales/.
https://www.c3.unam.mx/noticias/noticia174.html.
http://dof.gob.mx/nota_detalle.php?codigo=5606951&fecha=08/12/2020.
https://revistas.juridicas.unam.mx.
https://twitter.com/INAImexico/.
https://www.gob.mx/innovamx/articulos/inteligencia-artificial-131287.
https://openai.com/.
https://www.deepseek.com/.