

Inteligencia artificial y supervisión del fraude en los sistemas de seguridad social

Artificial Intelligence and Fraud Oversight in Social Security Systems

Inteligência artificial e supervisão da fraude nos sistemas de segurança social

Nermis Cesarina Andújar Troncoso*

Artículo de reflexión

Fecha de recepción: 8 de mayo de 2026

Fecha de aceptación: 17 de julio de 2026

Para citar este artículo:

Andújar Troncoso, N. C. (2026). Inteligencia artificial y supervisión del fraude en los sistemas de seguridad social. *Revista Análisis Jurídico-Político*, 8(16), 135-154. <https://doi.org/10.22490/26655489.11666>

RESUMEN

Históricamente, en los sistemas de seguridad social, el componente de salud ha sido blanco de prácticas ilícitas asociadas al fraude. Si bien son diversas las modalidades empleadas por los defraudadores, una de las más comunes consiste en acceder a la protección social ofrecida por un régimen de financiamiento que no se corresponde con la realidad socioeconómica, aportante o contributiva del presunto beneficiario. Esta desigualdad genera un déficit financiero en los ingresos recaudados al momento de su distribución, lo que afecta gravemente el equilibrio financiero del sistema y a sus verdaderos

* Abogada; especialista en Procedimiento Civil y en Dirección y Gestión de los Sistemas de Seguridad Social. Reconocida en la GC Powerlist: Latin America de The Legal 500 (ediciones 2022-2026). Cuenta con más de 20 años de trayectoria en el sector público. Actualmente, se desempeña como directora jurídica de la Tesorería de la Seguridad Social de la República Dominicana. Correos electrónicos: nandujartroncoso@gmail.com; nermis_andujar@tss.gob.do. ORCID: <https://orcid.org/0009-0004-7966-3647>

beneficiarios. Este artículo evalúa mejoras, métodos y oportunidades en los procesos operativos de los sistemas de seguridad social, con la finalidad de fortalecer la prevención y la detección oportuna del fraude mediante la implementación adecuada de los recursos que ofrecen las tecnologías de la información. La premisa fundamental se sostiene en que el fraude actúa como un mecanismo de evasión y elusión bastante eficaz y recurrente frente a los sistemas tradicionales de supervisión y control, los cuales, si bien funcionaron en su momento, han quedado obsoletos en un entorno digital caracterizado por desafíos constantes. En este contexto, la inteligencia artificial surge como una herramienta necesaria para equilibrar la balanza frente a las brechas oportunistas que mantienen expuestos a los sistemas. La metodología empleada es fundamentalmente cualitativa y comprende planteamientos, análisis y estudios de caso, complementados con algunos datos cuantitativos puntuales.

Palabras clave: administración pública; fraude; gobernanza digital; inteligencia artificial; seguridad social; supervisión automatizada.

ABSTRACT

Historically, the health component of social security systems has been a target of unlawful practices associated with fraud. Although fraudsters employ various methods, one of the most common consists of gaining access to the social protection provided by a financing scheme that does not correspond to the alleged beneficiary's socio-economic, contribution, or contributory status. This inequality creates a financial deficit in the revenues collected at the time of distribution, seriously affecting the system's financial balance of the system and its legitimate beneficiaries. This article evaluates improvements, methods, and opportunities within the operational processes of social security systems, aiming to strengthen fraud prevention and timely detection through the appropriate implementation of the resources offered by information technologies. The central premise is that fraud operates as a highly effective and recurrent mechanism of evasion and avoidance in the face of traditional supervision and control systems, which, although effective in the past, have become obsolete in a digital environment marked by constant challenges. In this context, artificial intelligence emerges as a necessary tool to restore

balance in the face of opportunistic gaps that leave these systems exposed. The methodology employed is primarily qualitative and includes approaches, analyses, and case studies, complemented by some specific quantitative data.

Keywords: artificial intelligence; automated supervision; digital governance; fraud; public administration; social security.

RESUMO

Historicamente, nos sistemas de seguridade social, o componente de saúde tem sido alvo de práticas ilícitas associadas à fraude. Embora sejam diversas as modalidades empregadas pelos infratores, uma das mais comuns consiste em obter acesso à proteção social oferecida por um regime de financiamento que não corresponde à realidade socioeconômica, contributiva ou de contribuição do suposto beneficiário. Essa desigualdade gera um déficit financeiro nas receitas arrecadadas no momento de sua distribuição, o que afeta gravemente o equilíbrio financeiro do sistema e os seus legítimos beneficiários. Este artigo avalia melhorias, métodos e oportunidades nos processos operacionais dos sistemas de seguridade social, com a finalidade de fortalecer a prevenção e a detecção oportuna da fraude por meio da implementação adequada dos recursos oferecidos pelas tecnologias da informação. A premissa fundamental sustenta que a fraude atua como um mecanismo de evasão e elisão bastante eficaz e recorrente diante dos sistemas tradicionais de supervisão e controle, os quais, embora tenham funcionado em seu momento, tornaram-se obsoletos em um ambiente digital caracterizado por desafios constantes. Nesse contexto, a inteligência artificial surge como uma ferramenta necessária para restabelecer o equilíbrio diante das brechas oportunistas que mantêm os sistemas expostos. A metodologia empregada é fundamentalmente qualitativa e compreende abordagens, análises e estudos de caso, complementados por alguns dados quantitativos pontuais.

Palavras-chave: administração pública; fraude; governança digital; inteligência artificial; seguridade social; supervisão automatizada.

1. INTRODUCCIÓN

El fraude es un tema controversial que empaña la finalidad y el objeto de cualquier sistema de protección social, ya que representa una amenaza para la estabilidad financiera, que es el eje de su viabilidad y sostenibilidad. Es importante comprender su concepción y las formas más comunes en que se materializa, así como el fin perseguido por sus actores, los beneficiarios destinatarios y, sobre todo, el gran desafío que supone para la administración pública no solo enfrentarlo, sino también detectarlo oportunamente y prevenirlo.

La sostenibilidad de los sistemas de protección social se enfrenta actualmente a desafíos estructurales que trascienden la gestión administrativa básica. Como señala la Organización Internacional del Trabajo (OIT, 2024) en su más reciente informe mundial, el fraude y la elusión no solo erosionan la base contributiva, sino que también comprometen el contrato social y la equidad intergeneracional.

En este contexto, autores como Montoya Melgar (2021) sostienen que la integridad del sistema es un requisito *sine qua non* para el ejercicio del derecho a la salud. El fraude, analizado por Barceló Moyano (2022) como un fenómeno sociojurídico, ha evolucionado hacia formas sofisticadas de simulación laboral, lo que exige que la administración adopte una postura proactiva.

Este artículo comprende un análisis del fenómeno del fraude desde una perspectiva sociojurídica y económica, así como de su impacto en el rol de supervisión de la administración pública. Asimismo, aborda la identificación de los tipos de fraude más frecuentes, las formas en que se materializan, el uso de prácticas dirigidas a evadir los controles en materia de supervisión y el aprovechamiento de oportunidades legales como mecanismo de elusión.

La intención es comprender mejor de qué manera la integración desistemas de inteligencia artificial permite superar las limitaciones de los modelos tradicionales de supervisión tradicionales para detectar y prevenir oportunamente las nuevas modalidades de fraude en los sistemas de protección social, preservar el equilibrio

financiero y garantizar la protección efectiva y progresiva de los beneficiarios reales de los sistemas de seguridad social.

Si bien se exploran los retos y desafíos que enfrentan los sistemas de protección social en la lucha contra el fraude y su persecución, también se proporciona información valiosa para la formulación de políticas públicas y procedimientos internos orientados al diseño de planes y estrategias que contribuyan a una prevención y un control más efectivos. Para ello, se propone una serie de acciones encaminadas a potenciar el rol de las entidades, impulsar el diseño de un esquema de control y supervisión acorde con los nuevos tiempos, apoyado en los avances tecnológicos, y fortalecer las estrategias robustas de coordinación, colaboración y cooperación entre los actores involucrados.

2. METODOLOGÍA

La metodología de la presente investigación se desarrolla desde un enfoque cualitativo de carácter sociojurídico y reflexivo, que articula tres funciones complementarias. La primera es diagnóstico-crítica y está orientada al análisis de las limitaciones de los modelos tradicionales de supervisión en los sistemas de seguridad social frente a las nuevas modalidades de fraude en entornos digitalizados. La segunda es descriptivo-comparada y se dirige a identificar y sistematizar las modalidades de fraude y las experiencias de implementación de herramientas de inteligencia artificial en distintas jurisdicciones. La tercera es propositivo-normativa y se enfoca en el diseño de una arquitectura de supervisión inteligente sustentada en garantías jurídicas. Esta triple aproximación integra el rigor jurídico con la visión estratégica de la gestión pública moderna.

La reflexión se sustenta en la revisión de documentación especializada, literatura académica, informes técnicos de organismos internacionales y experiencias comparadas relacionadas con la gobernanza pública, la sostenibilidad financiera y la transformación digital de las bases de datos en materia de seguridad social. La selección del corpus teórico privilegió fuentes que abordan de manera directa la intersección entre inteligencia artificial, administración pública y

control del fraude en los sistemas de protección social, con prioridad para los informes de organismos internacionales —OIT, Asociación Internacional de la Seguridad Social (AISS) y Organización para la Cooperación y el Desarrollo Económicos (OCDE)— y para la literatura jurídica y de gobernanza digital reciente.

En cuanto a los casos nacionales, se seleccionaron España, Estados Unidos y República Dominicana por tratarse de sistemas con experiencia documentada en la implementación de herramientas de inteligencia artificial para la supervisión del fraude y por su valor comparado frente al Sistema Dominicano de Seguridad Social, creado en 2001. Este último constituye el anclaje normativo primario a partir del cual se elabora el análisis, en atención al interés y a la experiencia del autor.

Finalmente, el trabajo propone una ruta orientada a la evolución de los mecanismos institucionales. Se plantea el diseño de estrategias basadas en la interoperabilidad de datos, la automatización de procesos y la supervisión inteligente. El objetivo es transitar de un modelo reactivo y manual hacia un ecosistema de detección temprana, fortalecer la capacidad de respuesta del Estado y garantizar la integridad de los recursos destinados a la seguridad social.

3. EVOLUCIÓN DE LOS MODELOS DE PROTECCIÓN SOCIAL Y EL SURGIMIENTO DE BRECHAS SISTÉMICAS

La transición de los sistemas de seguridad social desde el histórico modelo bismarckiano —basado en el aseguramiento del trabajador— hacia los modelos de protección social universal vigentes en la actualidad ha generado una complejidad administrativa sin precedentes. Esta evolución ha desplazado la supervisión y el control desde una inspección tradicional, física o basada en documentos, hacia la gestión de grandes bases de datos.

Es indudable que la robustez y la madurez de un sistema de seguridad social no solo se miden únicamente por su cobertura o por el nivel prestacional progresivo de sus prestaciones, sino también por su capacidad de resiliencia y respuesta frente a las “brechas oportunistas” aprovechadas mediante mecanismos fraudulentos.

Desafortunadamente, estas brechas surgen porque las normas legales y operativas suelen evolucionar con mayor lentitud que las tácticas empleadas por los defraudadores, lo que permite que la arquitectura digital de los sistemas, es decir, sus bases de datos, sea vulnerable a la manipulación de la información.

El fraude, además de constituir un hecho ilícito en el ámbito de los delitos económicos, supone una ruptura del pacto social por su impacto directo en la vulneración de derechos constitucionales enmarcados dentro de los derechos sociales o de tercera generación, como es el caso de la salud y la seguridad social.

Antes de continuar, resulta esencial establecer la diferencia técnica entre los siguientes términos:

- Fraude: engaño deliberado (por ejemplo, empresas fantasmas, de papel, ficticias o inoperantes).
- Evasión: incumplimiento total o parcial de la obligación de realizar aportes (por ejemplo, no registrar a los trabajadores, hacerlo de manera intermitente o reportar salarios o ingresos inferiores a los devengados para disminuir la carga porcentual de los aportes).
- Elusión: el aprovechamiento de “vacíos” o “espacios grises” en las normativas legales para pagar menos de lo debido, lo que configura una debilidad sistemática.

El impacto de este fenómeno en el equilibrio financiero de la protección social genera un claro efecto dominó: disminución de los ingresos por la fuga o evasión intencional de recursos; déficit prestacional; riesgo para los beneficiarios más vulnerables; e impedimento u obstaculización del principio de progresividad de los sistemas.

La lucha contra el fraude y la implementación de tecnologías disruptivas, como la inteligencia artificial, responden a lineamientos éticos alineados con los Objetivos de Desarrollo Sostenible (ODS). La integridad de los sistemas de protección social actúa como catalizadora de la Agenda 2030 (Naciones Unidas, 2015): la lucha contra el fraude protege la cobertura universal de salud y reduce las desigualdades (ODS 3 y 10); defiende el trabajo decente al combatir la informalidad y la subdeclaración (ODS 8); impulsa la modernización institucional, la transparencia y la lucha contra la corrupción

(ODS 9 y 16); y fomenta el intercambio de datos y de modelos exitosos de supervisión exitosos entre los Estados (ODS 17). Por lo tanto, la prevención del fraude mediante inteligencia artificial no constituye una decisión meramente técnica, sino un compromiso con la justicia social y la sostenibilidad financiera del sistema.

En esta línea global, el Convenio 102 de la Organización Internacional del Trabajo (OIT, 1952) establece los pilares de la protección social moderna. Estos principios exigen la responsabilidad general del Estado en la administración eficiente y la sostenibilidad financiera mediante el equilibrio actuarial. Para garantizar la universalidad y la integralidad de las prestaciones, resulta imperativo proteger la solidaridad del sistema. En este sentido, la lucha contra el fraude mediante tecnologías avanzadas no constituye únicamente una medida administrativa, sino también un mecanismo para asegurar que los recursos se distribuyan con criterios de igualdad de trato y con la participación de los sectores protegidos en la preservación de su patrimonio común.

4. DE LA EVASIÓN TRADICIONAL DE PAGO A LA SIMULACIÓN DE RELACIÓN LABORAL

El fraude en la seguridad social ha evolucionado desde la simple omisión de pago—evasión—hacia formas sofisticadas de simulación jurídica. Tal es el caso de empresas que simulan relaciones laborales mediante la creación de sociedades comerciales ficticias, registradas en la seguridad social con la finalidad de reportar supuestos trabajadores para que estos, a cambio de un pago a un tercero, puedan recibir los diversos beneficios del sistema, especialmente el seguro de salud, por ser el de necesidad y acceso más inmediatos.

Incluso algunas empresas que desarrollan una actividad comercial legítima acceden a comercializar la cobertura en salud como si se tratara de un seguro privado, aunque dentro del marco de los sistemas de seguridad social. Para ello, registran como trabajadores a personas interesadas, a cambio de un beneficio económico para el “empleador” por concepto del servicio prestado. Este *modus operandi* puede ser desconocido por los beneficiarios, pues quienes

lo ejecutan suelen presentarse como promotores o representantes de seguros de salud (Ortiz, 2023).

Para Barceló Moyano (2018), el fraude en las prestaciones de la seguridad social admite dos modalidades típicas: la obtención ilícita inicial de una prestación —por ejemplo, del seguro de desempleo o de incapacidad— y la prolongación indebida de una prestación obtenida originalmente de forma lícita, como ocurre cuando se mantiene una pensión de viudedad pese a haber contraído un nuevo matrimonio. Frente a este segundo supuesto, el autor destaca que exigir periódicamente una “prueba de vida” al pensionista contribuye a evitar el gasto derivado del fraude y el detrimento de las finanzas del sistema (Barceló Moyano, 2018, p. 64).

De manera similar a este último ejemplo, se encuentran quienes reciben prestaciones del seguro de desempleo mientras ejercen de forma oculta una actividad por cuenta ajena oculta o trabajan como autónomos, percibiendo ingresos sin reportarlos ni declararlos. También se incluyen quienes reciben prestaciones por algún tipo de incapacidad temporal cuando, en realidad, se encuentran aptos para trabajar.

Para la Social Security Administration de los Estados Unidos, el fraude consiste en obtener algo de valor mediante una representación falsa o en ocultar un hecho relevante que deba utilizarse para determinar los beneficios y pagos correspondientes. Como ejemplos de fraude, además de los citados previamente, esta entidad enumera los siguientes: formular declaraciones falsas en las reclamaciones; utilizar indebidamente los beneficios por parte de otra persona; no reportar el fallecimiento de un familiar y continuar recibiendo sus beneficios; comprar o vender tarjetas del Seguro Social; presentar reclamaciones mediante la identidad de otra persona; estafar a terceros haciéndose pasar por empleado del Seguro Social; o sobornar a sus empleados del seguro social (Social Security Administration USA, s. f.).

En estos casos, un desafío importante para la administración pública radica en la asimetría de la información, dada la dificultad de validar, en tiempo real y de forma masiva, mediante cruces de datos interinstitucionales, elementos esenciales como la veracidad

de una relación laboral, los pagos salariales realizados fuera de un entorno digital trazable y la documentación societaria, frente a millones de registros digitales.

Un ejemplo de cooperación interinstitucional se observa en la Tesorería General de la Seguridad Social de España, que mantiene, desde 2009, un intercambio recíproco de información tributaria y de gestión recaudatoria. Este mecanismo permite identificar y comprobar la facturación para detectar figuras ilícitas, como los falsos autónomos (Organización Iberoamericana de Seguridad Social [OISS], 2019).

Por otro lado, y no menos importante, se configura el denominado fraude interno, que consiste básicamente en actos de corrupción. Este tipo de fraude involucra a empleados o funcionarios de las entidades que conforman los sistemas de seguridad social, quienes, debido a las funciones que ejercen, tienen acceso a información y procesos que pueden manipular para obtener beneficios personales o favorecer a terceros. También comprende a los prestadores de servicios, tal y como lo ilustra Montoya Vega (2019) mediante el testimonio de un médico que admite ordenar exámenes “quizá innecesarios” a cambio de una comisión del laboratorio, o contratar a extranjeros pagándoles menos del salario mínimo vital. Según este testimonio, el fraude permea prácticamente todos los espacios de un sistema concebido para un fin tan noble como la protección social (Montoya Vega, 2019, p. 64).

En este sentido, la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2023) recomienda que la transformación digital de los servicios de salud priorice la trazabilidad financiera para combatir la corrupción.

Asimismo, Santos (2018) plantea que el fraude no es un secreto para nadie y señala que, en la seguridad social, especialmente en los servicios de salud, adopta múltiples modalidades que involucran a los distintos sectores representados en el sistema, tales como: centros médicos, médicos independientes, centros de diagnóstico y centros especializados.

5. IMPACTO EN LA SOSTENIBILIDAD Y DESAFÍOS CRÍTICOS EN LA GESTIÓN DE SUPERVISIÓN

El fraude erosiona los ingresos recaudados y provoca un déficit que compromete la progresividad de los derechos sociales, principio fundamental de la protección social. La judicialización *post-facto* —perseguir el fraude una vez cometido— resulta financieramente ineficiente debido a los altos costos procesales, la mora judicial y la baja tasa de recuperación de los fondos, mientras la dinámica defraudadora crece y avanza.

Por lo tanto, los resultados de este análisis sugieren que la sostenibilidad del sistema depende de una transición hacia modelos de prevención activa. Es aquí donde la tecnología de la información deja de ser un repositorio de datos para convertirse en un instrumento de vigilancia, sentando las bases para la implementación de herramientas de inteligencia artificial, como se verá más adelante.

En el caso de España, García Delgado (2018) recoge, con base en cifras oficiales citadas en su estudio, algunas estadísticas sobre los déficits ocasionados por el fraude a la seguridad social. Según refiere el autor, en el marco de un plan de lucha contra el empleo irregular desarrollado en 2012, se detectaron cerca de medio millón de empleos irregulares y 6500 empresas ficticias, y se convirtieron en indefinidos 320 000 contratos reportados como temporales, con un impacto económico estimado en 19 700 millones de euros. El autor añade que, entre 2013 y 2015, el Buzón de Lucha contra el Fraude Laboral recibió 135 250 denuncias anónimas, de las cuales la inspección inició actuaciones en 72 545 casos (García Delgado, 2018, pp. 253-265).

En ese sentido, Vargas (2017), en representación de la Asociación Dominicana de Administradoras de Riesgos de Salud (ADARS) —gremio que agrupa al sector de la salud en la República Dominicana— ha manifestado con frecuencia, en sus entrevistas, una profunda preocupación por los fraudes derivados de afiliaciones y traspasos irregulares.

En esa misma línea, Vargas (2017) también denunció que los fraudes representarían aproximadamente entre el 10 % y el 15 % de los pagos realizados por las administradoras de riesgos de salud (ARS) —cifra estimada por el gremio— como resultado de prácticas realizadas por los prestadores, entre ellos los centros clínicos y los médicos afiliados al sistema, para obtener pagos que no corresponden con la realidad del afiliado. Entre estas modalidades se encuentran la indicación de medicamentos de costo elevado en lugar de sus componentes genéricos, así como la realización de intervenciones quirúrgicas que podrían evitarse mediante otros procedimientos no invasivos.

El consultor especialista en seguridad social Díaz Santana (2022) también se refirió a los casos de fraude contra Medicare y Medicaid en Estados Unidos, que generaron pérdidas de entre el 3 % y el 10 % del gasto en salud. Estos casos involucran a proveedores de servicios de salud, equipos médicos y medicamentos que no son suministrados o cuyos costos son inflados.

La lucha contra el fraude en la seguridad social no solo enfrenta los sofisticados mecanismos de actuación de los infractores, sino también una serie de barreras estructurales que limitan la capacidad de respuesta institucional. El principal obstáculo radica en la asimetría tecnológica y en las barreras que enfrenta la administración pública durante la transición hacia la automatización, debido a la rigidez presupuestaria y a la falta de personal altamente calificado en análisis de datos.

Siguiendo las directrices de la Asociación Internacional de la Seguridad Social (AISS, 2023), la interoperabilidad de los datos y la supervisión automatizada se presentan como la arquitectura de integridad necesaria para equilibrar la balanza frente a las brechas oportunistas (Noveck, 2021). En este sentido, Bustamante (2021) destaca que la interoperabilidad entre las bases de datos fiscales y las de seguridad social constituye un factor determinante para reducir las brechas de información que aprovechan los defraudadores.

Estudios recientes sobre gobernanza digital (Gascó-Hernández, 2024) sugieren que el éxito de estas herramientas radica en la capacitación continua del personal jurídico y técnico encargado de interpretar los resultados del sistema.

Por otro lado, también influyen significativamente las debilidades en la integridad y el intercambio de datos, la fragmentación de la información, la falta de estándares de interoperabilidad entre los organismos gubernamentales y el uso de plataformas vulnerables a ataques de ciberseguridad. Estas circunstancias generan “silos de información” que son aprovechados por los defraudadores para evitar su detección.

A esto se suma la necesidad de equilibrar la supervisión administrativa con normativas de protección de datos personales cada vez más robustas y restrictivas, que exigen sustentarla en principios éticos. Esto implica diseñar protocolos de asistencia técnica y jurídica que permitan una colaboración interinstitucional fluida, sin vulnerar los derechos fundamentales.

En ocasiones, la propia legislación impone obstáculos al no otorgar facultades suficientes de actuación para realizar intervenciones preventivas sin necesidad de una judicialización anterior que, por su naturaleza, prolonga los tiempos de actuación oportuna. Asimismo, existe el riesgo de normalizar el fraude bajo un esquema de aceptación mínima, derivado de comparar el costo-beneficio de una actuación compleja y prolongada con el resultado tardío.

En este sentido, la capacidad predictiva de los sistemas de seguridad social no constituye únicamente una opción técnica, sino una necesidad para la supervivencia de estos. Como argumentan Flynn y Williams (2024), la analítica predictiva es la barrera más efectiva contra el fraude complejo en el ámbito de la salud.

El uso de las tecnologías de la información y la comunicación en el tratamiento de datos en la administración pública debe, desde su concepción, alinearse con la normativa aplicable en cada Estado, con el fin de legitimar su implementación. En este sentido, Valero Torrijos (2019) sostiene que los sistemas basados en *machine learning* no solo requieren una aprobación jurídica inicial, sino también “sistemas de evaluación periódicos” que permitan verificar que su evolución algorítmica continúa ajustándose a las premisas originales o que, en su defecto, estas sean actualizadas en consecuencia (Valero Torrijos, 2019, p. 91).

6. LA CONVERGENCIA ENTRE *BIG DATA* Y EL APRENDIZAJE AUTOMÁTICO

La transición hacia una supervisión inteligente no debe entenderse como el simple reemplazo de los procesos manuales, sino como una forma de “gestión pública inteligente” (Criado, 2021). La implementación de algoritmos de aprendizaje automático permite identificar patrones de riesgo invisibles para la auditoría tradicional; sin embargo, esta transformación debe estar respaldada por garantías jurídicas.

El primer paso hacia una supervisión moderna consiste en reconocer que la información no es solo un registro, sino un activo estratégico con un alto potencial. La implementación de una infraestructura de *big data* permite procesar la velocidad, el volumen y la variedad de las transacciones en los sistemas de seguridad social.

6.1. LA IA PARA LA TOMA DE DECISIONES

El uso de algoritmos sofisticados permite interpretar grandes volúmenes de datos y puede contribuir a mitigar ciertos sesgos y márgenes de discrecionalidad presentes en la revisión manual. Sin embargo, esta mitigación no es automática ni absoluta, pues depende de un diseño algorítmico auditable y de una supervisión humana constante, en consonancia con las garantías de transparencia y debido proceso que se desarrollan más adelante.

6.2. EL APRENDIZAJE AUTOMÁTICO PARA EL REFINAMIENTO DE LA CALIDAD

El aprendizaje automático no solo permite detectar el fraude, sino que también actúa como un mecanismo de depuración y estandarización. Al identificar duplicados, inconsistencias y errores en los registros, la inteligencia artificial puede contribuir a preservar la integridad de las bases de datos, lo que favorece una toma de decisiones informada y eficiente.

6.3. LA SUPERVISIÓN BASADA EN RIESGOS (SBR) Y EL PERFILAMIENTO DINÁMICO DEL EMPLEADOR

Este modelo se inspira en el éxito de la administración tributaria y representa un ecosistema dinámico de datos para la toma de decisiones. Sus componentes principales son los siguientes:

- Variables de análisis: la integración de microdatos provenientes de patrones societarios, rotación inusual de personal, cambios abruptos en los balances financieros y sectores económicos con alta informalidad.
- Matriz de riesgo: el sistema debe asignar niveles de riesgo —bajo, moderado y alto— basados no necesariamente en función del tamaño de la empresa, sino de su comportamiento. Una gran empresa puede representar un riesgo bajo, mientras que las microempresas pueden constituir focos críticos de simulación laboral.
- Alertas automatizadas: la generación de alertas en tiempo real permite una fiscalización preventiva, al facilitar la actuación antes de que el daño financiero al sistema sea irreversible.

La efectividad de la supervisión basada en riesgos no depende únicamente de la capacidad del algoritmo, sino también de la calidad y la ética en el tratamiento de los datos masivos. Al respecto, Mayer-Schönberger y Cukier (2022) señalan que el análisis de *big data* permite identificar correlaciones que la observación humana suele omitir, lo cual resulta fundamental para detectar la elusión contributiva. No obstante, para que estos sistemas sean sostenibles, deben integrarse en un marco de transparencia proactiva (Hofmann *et al.*, 2023), de modo que la automatización no vulnere el debido proceso administrativo.

6.4. IDENTIFICACIÓN BIOMÉTRICA Y TRAZABILIDAD DEL INDIVIDUO

Para combatir la suplantación de identidad y las “empresas fantasmas”, la biometría —fisiológica y conductual— constituye una de las herramientas más robustas de verificación disponibles, sin que ello implique una solución definitiva o exenta de riesgos. Su uso

debe sujetarse a los mismos principios de proporcionalidad, minimización de datos y debido proceso que rigen el resto del modelo de supervisión inteligente. Al registrar características identitarias únicas, contribuye a garantizar que el beneficiario de la prestación sea realmente la persona reportada por el empleador, lo que permite fortalecer el sistema frente a los fraudes derivados de afiliaciones múltiples o inexistentes, siempre bajo controles que eviten un uso desproporcionado de datos sensibles.

6.5. ÉTICA, RETROALIMENTACIÓN Y DEBIDO PROCESO

Un modelo de inteligencia artificial aplicado en la administración pública debe ser transparente. Como Estado garantista, la administración debe velar por que el administrado comprenda los criterios utilizados para determinar su perfil de riesgo y pueda adoptar acciones orientadas a modificarlo. Esto no solo genera confianza y fortalece la reputación administrativa, sino que también fomenta una cultura de *compliance* colaborativo.

Al respecto, Valero Torrijos (2022) advierte que la gobernanza algorítmica debe respetar los principios de transparencia y explicabilidad. En este sentido, Pasquale (2022) alerta sobre los riesgos de los sistemas algorítmicos opacos o de “caja negra”, cuyos criterios de decisión resultan inaccesibles para los propios administrados, lo que refuerza la necesidad de establecer mecanismos de explicabilidad y auditoría constante.

7. CASOS DE IMPLEMENTACIÓN: LA IA APLICADA

7.1. ESPAÑA: EL SISTEMA INSS Y LA INSPECCIÓN DE TRABAJO

El Instituto Nacional de la Seguridad Social (INSS) de España utiliza algoritmos desde 2018 para gestionar y controlar las bajas laborales mediante el denominado Modelo de Priorización de Citas, que determina qué expedientes deben revisar primero los médicos inspectores con base en predicciones algorítmicas. Asimismo, desde

2015, la Dirección General de la Inspección de Trabajo y Seguridad Social utiliza un *software* basado en inteligencia artificial para identificar el fraude con mayor agilidad y orientar las inspecciones desde un enfoque aleatorio hacia uno predictivo sustentado en datos (Casal Tavasci, 2025; Revista Seguridad Social, 2018).

7.2. ESTADOS UNIDOS DE AMÉRICA: CMS MEDICARE/MEDICAID

Los Centers for Medicare & Medicaid Services (CMS) de los Estados Unidos implementaron un sistema de detección de fraude basado en inteligencia artificial que, según declaraciones de funcionarios de la agencia recogidas por la prensa especializada, generó ahorros reportados por 2000 millones de dólares en aproximadamente un año, con una precisión superior al 90 % en la identificación de reclamaciones sospechosas (Goode, 2026). Esta cifra también ha sido difundida por contratistas del sector (General Dynamics Information Technology, s. f.), por lo que se recomienda verificarla mediante los informes oficiales del propio CMS. Una condición central del modelo consiste en mantener un “humano en el circuito” para revisar las alertas de riesgo antes de suspender los pagos, con el fin de garantizar que se evalúe el contexto clínico y administrativo completo (Trewin, 2025).

8. CONCLUSIONES

El recorrido analítico de este artículo permite identificar que los sistemas de seguridad social enfrentan actualmente una disyuntiva estructural: continuar gestionando el fraude de forma reactiva, con el costo financiero y social que ello implica, o asumir la transformación digital como una apuesta institucional de fondo. La investigación muestra que las modalidades de fraude han superado con creces la capacidad de respuesta de los modelos tradicionales de supervisión, lo que afecta simultáneamente la sostenibilidad actuarial del sistema, la calidad de las prestaciones destinadas a los beneficiarios reales y la integridad del mercado de servicios de salud.

En este contexto, la inteligencia artificial y el aprendizaje automático emergen no como lujos tecnológicos, sino como la respuesta institucional más coherente frente a defraudadores que operan con una sofisticación creciente. La supervisión basada en riesgos, la interoperabilidad de datos y la identificación biométrica no reemplazan la función pública, sino que la dotan de la capacidad predictiva que demandan los entornos digitales. Para que esta transición sea legítima y sostenible, debe estar acompañada de marcos normativos claros, auditoría humana de los algoritmos y una cultura institucional de cumplimiento colaborativo.

En consecuencia, surge el reto de transformar los “silos de información” en un ecosistema de datos compartidos entre las entidades del Estado. La trazabilidad de los registros no solo debe constituir un ejercicio contable, sino también una herramienta de inteligencia estratégica que permita transitar de una gestión reactiva e ineficiente hacia una prevención inteligente.

Como reflexión final sobre la protección social, el fortalecimiento de las funciones de supervisión y la lucha contra la corrupción interna y externa son imperativos para preservar el pacto social. La capacidad de un Estado para proteger a sus ciudadanos frente a contingencias de salud depende directamente de su habilidad para blindar sus sistemas financieros contra el engaño. En este sentido, la prevención constituye la inversión más rentable para garantizar que la protección social sea, a largo plazo, un derecho universal, efectivo y sostenible.

Debido a las limitaciones de este trabajo —centrado en fuentes secundarias y en un análisis de carácter reflexivo—, se abre la puerta a futuras investigaciones que, mediante datos primarios y estudios comparados entre sistemas nacionales, permitan medir el impacto real de estas herramientas en la reducción del fraude y en la recuperación de recursos para los verdaderos beneficiarios.

La protección social es, en esencia, un pacto de solidaridad intergeneracional. Blindar ese pacto contra el fraude constituye tanto una obligación ética del Estado como la inversión de mayor rentabilidad social a largo plazo.

REFERENCIAS

- Asociación Internacional de la Seguridad Social. (2023). *Guías de la AISS sobre la solución de errores, la evasión y el fraude en los sistemas de seguridad social*. <https://www.issa.int/es/guidelines/eef/180194>
- Barceló Moyano, M. (2018). El fraude de prestaciones de la seguridad social: modalidades típicas. *Revista de Derecho Administrativo*, 12(1), 58–75.
- Barceló Moyano, M. (2022). La lucha contra el fraude en la seguridad social: Nuevas perspectivas jurídicas. *Revista de Derecho Administrativo*, 14(2), 45–68.
- Bustamante, R. (2021). Interoperabilidad y gestión de datos en la administración pública iberoamericana. *Revista Digital de Derecho Administrativo*, (25), 115–139. <https://doi.org/10.18601/21452946.n25.06>
- Casal Tavasci, J. (2025, 19 de diciembre). Inspección de Trabajo y Seguridad Social usará la inteligencia artificial. *Protección Data*. <https://protecciondata.es/uso-robots-inspeccion-trabajo/>
- Criado, J. I. (2021). Inteligencia artificial y administración pública: Hacia una gestión pública inteligente. *Revista del CLAD Reforma y Democracia*, (78), 5–38.
- Díaz Santana, A. (2022, 7 de abril). *EEUU: Fraudes millonarios de médicos dominicanos*. ADARS. <https://adars.org.do/eeuu-fraudes-millonarios-de-medicos-dominicanos-por-arismendi-diaz-santana/>
- Flynn, K. y Williams, J. (2024). *Combating healthcare fraud through predictive analytics: A global perspective*. Oxford University Press.
- García Delgado, J. L. (2018). La lucha contra el fraude en la seguridad social en el marco de los nuevos principios de actuación de la administración pública. *APOSTA Revista de Ciencias Sociales*, 235–256.
- Gascó-Hernández, M. (2024). *The intelligent government: AI and the future of public administration*. Routledge.
- General Dynamics Information Technology. (s. f.). *Centers for Medicare and Medicaid (CMS)*. GDIT. <https://www.gdit.com/industries/health/centers-for-medicare-and-medicare-cms/>
- Goode, D. (2026, 24 de febrero). *CMS saved \$2 billion by using AI to fight fraud, official says*. Nextgov/FCW. <https://www.nextgov.com/artificial-intelligence/2026/02/cms-saved-2-billion-using-ai-fight-fraud-official-says/411661/>
- Hofmann, S., Carneiro, L. y Becker, J. (2023). Artificial intelligence in the public sector: A systematic literature review. *Government Information Quarterly*, 40(3), 101–124.
- Mayer-Schönberger, V. y Cukier, K. (2022). *Big data: La revolución de los datos masivos*. Turner Noema.
- Montoya Melgar, A. (2021). *Derecho de la seguridad social* (22.ª ed.). Tecnos.
- Montoya Vega, R. (2019, 24 de octubre). La corrupción no soy yo. *Diario Expreso de Ecuador*. <https://www.expreso.ec/actualidad/corrupcion-19085.html>
- Naciones Unidas. (2015). *Transformar nuestro mundo: La Agenda 2030 para el desarrollo sostenible*. https://unctad.org/system/files/official-document/ares70d1_es.pdf

- Noveck, B. S. (2021). *Smart citizens, smarter state: The technologies of expertise and the future of governing*. Harvard University Press.
- Organización Iberoamericana de Seguridad Social. (2019). *Líneas de actuación de la Tesorería General de la Seguridad Social española para la prevención y corrección del fraude*. <https://oiss.org/wp-content/uploads/2019/10/L%C3%ADneas-de-actuaci%C3%B3n-de-la-Tesorer%C3%ADa-General-de-la-Seguridad-Social-espa%C3%B1ola-para-la-prevenci%C3%B3n-y-correcci%C3%B3n-del-fraude.pdf>
- Organización Internacional del Trabajo. (1952). *Convenio sobre la seguridad social (norma mínima)*, 1952 (núm. 102). https://www.ilo.org/dyn/normlex/es/?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:312247
- Organización Internacional del Trabajo. (2024). *Informe mundial sobre la protección social 2024-2026: Universalizar la protección social para la justicia social*. OIT. <https://www.ilo.org/es/publications/flagship-reports/informe-mundial-sobre-la-proteccion-social-2024-2026-proteccion-social>
- Organización para la Cooperación y el Desarrollo Económicos. (2023). *Government at a glance 2023*. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/06/government-at-a-glance-2023_da193b0d/3d5c5d31-en.pdf
- Ortiz, A. (2023, 4 de mayo). TSS ha dado baja a 34 mil por fraudes a sistema. *El País*. <https://hoy.com.do/tss-ha-dado-baja-a-34-mil-por-fraudes-a-sistema/>
- Pasquale, F. (2022). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Revista Seguridad Social. (2018, 1 de junio). Big data contra el fraude. Ministerio de Inclusión, Seguridad Social y Migraciones. <https://revista.seg-social.es/-/big-data-contra-el-fraude/>
- Santos, M. D. (2018, 18 de febrero). Fraudes en el Sistema Dominicano de salud. *Diario Salud*. <https://www.diariosalud.do/articulos/fraudes-comunes-de-la-atencion-en-salud-en-el-sistema-dominicano-de-seguridad-social/>
- Social Security Administration USA. (s. f.). Prevención y Reporte de Fraude. Tomamos el fraude en serio y usted también debería hacerlo. <https://www.ssa.gov/espanol/fraude/>
- Trewin, A. (2025, 23 de diciembre). *CMS uses explainable AI to strengthen Medicare fraud detection*. GovCIO Media & Research. <https://govciomedia.com/cms-uses-explainable-ai-to-strengthen-medicare-fraud-detection/>
- Valero Torrijos, J. (2019). Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. *Revista Catalana de Dret Públic*, (58), 82–96. <https://doi.org/10.2436/rcdp.i58.2019.3307>
- Valero Torrijos, J. (2022). Las garantías jurídicas de la inteligencia artificial en la actividad administrativa. *Revista de Administración Pública*, (218), 75–104.
- Vargas, J. M. (2017, 14 de diciembre). ADARS pide a autoridades tomen medidas para enfrentar mafias. *Diario Salud*. <https://www.diariosalud.do/ars/adars-pide-a-autoridades-tomen-medidas-para-enfrentar-mafias/>