INFORME 1/2025

APROXIMACIÓN A LAS POSIBILIDADES DE LA INTELIGENCIA ARTIFICIAL (IA) EN LA LUCHA CONTRA EL FRAUDE Y LA CORRUPCIÓN. SECTOR PÚBLICO LOCAL.

1.-Introducción

La presencia habitual de referencias a las Inteligencia Artificial (IA) ha hecho que nos familiaricemos con ella, quedando implantada de manera definitiva en nuestra cotidianidad. Su potencialidad y afección a nuestras vidas son indiscutibles, formando parte de nuestra realidad más inmediata. Su uso está implantado, o comenzando a hacerlo, en distintos sectores y servicios, entre los que se encuentran las Administraciones Públicas.

Un punto de partida para una aproximación a la denominación IA sería la búsqueda de una posible definición del concepto, y si bien es complejo definirla, y no existe una definición formalmente aceptada internacionalmente, podemos utilizar como inicio el marco jurídico que nos otorga el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial. El artículo 3, bajo la denominación "definiciones", señala que:

A los efectos del presente Reglamento, se entenderá por: 1) «sistema de IA»: un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

El objetivo del Reglamento es mejorar el funcionamiento del mercado interior mediante el establecimiento de un marco jurídico uniforme para el desarrollo, la puesta en servicio y la utilización de sistemas de inteligencia artificial en la Unión, de conformidad con los valores de la Unión.

Con el establecimiento de reglas se busca una IA *centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea.*

En los Considerandos del Reglamento se pone de manifiesto que la IA contribuye a generar *beneficios económicos, medioambientales y sociales muy diversos en todos los sectores económicos y las actividades sociales.* Y su uso *puede proporcionar ventajas competitivas esenciales a las empresas y facilitar la obtención de resultados positivos desde el punto de vista social y medioambiental* en distintos y numerosos ámbitos. Si bien, añade que *dependiendo de las circunstancias relativas a su aplicación, utilización y nivel de desarrollo tecnológico concreto, la IA puede generar riesgos y menoscabar los intereses públicos y los derechos fundamentales que protege el Derecho de la Unión.*

Por ello, el Reglamento establece normas comunes para los sistemas de IA al objeto de garantizar un *nivel elevado y coherente* de protección de los intereses públicos.

2.-Evolución en las normas que rigen la actuación tecnológica del sector público

Las Administraciones Públicas han sido desde hace años permeables a las innovaciones tecnológicas, incorporándolas a su gestión y procesos, si bien con las características propias del derecho administrativo. Transitando desde una administración electrónica a una digital para llegar a la situación actual con una presencia cada vez mayor de la IA:

-Con la administración electrónica, las tecnologías de la información y la comunicación (TIC) se utilizan en la gestión administrativa, mejorando su funcionamiento.

-Con la administración digital se amplía ese uso de las tecnologías de una manera más integral en la prestación de servicios y acceso a datos aportando un mayor valor público (OCDE, 2014. Recomendación sobre Estrategias de Gobierno Digital).

-Con la IA los sistemas operan con elementos de autonomía basándose en datos obtenidos de humanos o de máquinas y genera contenidos, recomendaciones o decisiones.

La ya derogada Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en su preámbulo, se pronunciaba así: *Las técnicas burocráticas formalistas, supuestamente garantistas, han caducado, por más que a algunos les parezcan inamovibles, y la Ley se abre decididamente a la tecnificación y modernización de la actuación administrativa en su vertiente de producción jurídica y a la adaptación permanente al ritmo de las innovaciones tecnológicas.*

Hace ya casi dos décadas nació la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que respondía a *las nuevas realidades, exigencias y experiencias que se habían puesto de manifiesto, al propio desarrollo de la sociedad de la información y al cambio de circunstancias tecnológicas y sociales, entre otros factores, reconocía el derecho de la ciudadanía a relacionarse electrónicamente con las Administraciones Públicas*. Y ya abogaba por la obligación de que dichas Administraciones impulsaran el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias.

Posteriormente, otras leyes han atendido a la necesidad y demanda de que la tramitación electrónica constituyera la actuación habitual de las Administraciones Públicas. En este sentido, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Este último texto legal, en su artículo 41, regula y define la actuación administrativa automatizada:

1. Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público.

2. En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente.

Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

Más recientemente, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, se manifiesta, en su preámbulo, en los siguientes términos:

Los cambios que se están produciendo con la maduración de tecnologías disruptivas y su aplicación a la gestión de la información y la ejecución de políticas públicas, los nuevos modelos de relación de la ciudadanía y empresas con las Administraciones y la reutilización eficiente de la información son grandes desafíos que para ser afrontados con éxito y para que coadyuven a la Transformación digital exigen como presupuesto contar con un marco regulatorio adecuado, tanto con rango de ley como con rango reglamentario, que garantizando la seguridad jurídica para todos los intervinientes sirva a los objetivos de mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada, incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica y garantizar servicios digitales fácilmente utilizables.

El objeto del mencionado Reglamento, según su artículo 1º, es el desarrollo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en lo referido a la actuación y el funcionamiento electrónico del sector público.

En campos específicos como la contratación pública, es de significarse, dentro de los objetivos de la Estrategia Nacional de Contratación Pública, el artículo 334.2.d) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, en el que se dispone: *generalizar la contratación electrónica en todas las fases del procedimiento*.

La evolución de los sistemas de IA ha sorprendido por la rapidez en su desarrollo, y la adaptación de los procedimientos administrativos (o a la inversa) a estas nuevas herramientas con las debidas e imprescindibles garantías y se plantea, sin duda, como un reto jurídico de gran calado.

Son muchas las nuevas oportunidades que nos ofrece la IA, pero estas van acompañadas de numerosos riesgos en materias tan sensibles como la protección de datos o derechos fundamentales.

3.-La nueva regulación de la Unión Europea

El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, es pionero mundial en establecer un marco jurídico sobre IA.

Será aplicable a partir del 2 de agosto de 2026 (artículo 113), contemplándose para su aplicabilidad los siguientes hitos temporales: el 2 de febrero de 2025 han entrado en vigor las prohibiciones y las obligaciones de alfabetización; y las obligaciones relativas a modelos IA de uso general y las normas de gobernanza se

aplicarán a partir de 2 de agosto de 2025; y la regulación de los sistemas de alto riesgo tienen un régimen transitorio ampliado al 2 de agosto de 2027.

Como aspectos destacados de este Reglamento podemos hacer referencia a los siguientes:

Se definen cuatro niveles de riesgo de los sistemas IA: riesgo mínimo, riesgo específico de transparencia, riesgo alto y riesgo inaceptable. Se prohíben las aplicaciones y sistemas que supongan un riesgo inaceptable. El Capitulo II recoge las prácticas prohibidas de la IA, entre las que se incluyen aquellas que utilicen técnicas subliminales para distorsionar el comportamiento de las personas que puedan causarles daños, o aquellas que usen vulnerabilidades de grupos específicos de personas, y también se impide la identificación biométrica en tiempo real en lugares accesibles al público, con la salvedad de los casos expresamente contenidos, tales como búsqueda de víctimas potenciales de delitos, prevención de amenazas sobre infraestructuras o personas físicas, ataques terroristas o persecución de crímenes punibles con más de cinco años de privación de libertad.

La mayoría de los sistemas de IA que actualmente se utilizan en Europa se consideran de riesgo mínimo, tales como sistemas de recomendaciones, filtros de correos no deseados, videojuegos.

Los proveedores deberán garantizar que las personas físicas sean informadas de que están interactuando con un sistema IA, y los que produzcan imágenes o sonidos que constituyan una ultra suplantación, pareciendo en verdad personas, lugares, objetos, deberán informar de ello, con las excepciones vinculadas a persecución del crimen o cuando se trate de contenidos que formen parte de una obra o programa manifiestamente creativos, satíricos, artísticos, de ficción o análogos.

La previsión de espacios controlados de pruebas para la IA, que proporcionarán las autoridades nacionales, en un entorno que fomente la innovación y facilite el desarrollo y validación de los sistemas IA, se establece en el Capítulo VI del Reglamento, bajo el epígrafe "Medidas de apoyo a la innovación". En estos espacios las autoridades competentes procurarán orientación, supervisión y apoyo con vistas a determinar los riesgos, en particular para los derechos fundamentales, la salud y la seguridad, a las pruebas y a las medidas de reducción y su eficacia en relación con las obligaciones y los requisitos de la ley.

Se establece la creación y estructura de un Consejo Europeo de Inteligencia Artificial con representantes de cada uno de los Estados miembros. Este Consejo prestará asesoramiento y asistencia a la Comisión y a los Estados miembros para facilitar la aplicación del Reglamento. La Comisión desarrollará sus capacidades en el ámbito de la IA mediante la Oficina de IA. La Comisión estará asistida por un Comité.

Importante es la obligación que se impone a los Estados miembros de designar, al menos, una autoridad notificante y una autoridad de vigilancia en relación con el Reglamento.

La Oficina de IA y los Estados miembros facilitarán la elaboración de códigos de conducta destinados a fomentar la aplicación voluntaria, de alguno o de todos los requisitos establecidos en el Reglamento para los sistemas de alto riesgo, a los sistemas de IA que no sean de alto riesgo, teniendo en cuenta las soluciones técnicas disponibles y las mejores prácticas del sector. Estos códigos podrán redactarlos los proveedores o responsables del despliegue de sistemas de IA particulares, las organizaciones que los representen o por ambos, y también con

participación de cualquier parte interesada y sus organizaciones representativas, como, por ejemplo, las organizaciones de la sociedad civil y el mundo académico.

La confidencialidad de la información y los datos obtenidos habrán de quedar garantizados, y así se establece en el articulado del Reglamento.

El régimen de sanciones y multas queda contemplado en el Capítulo XII.

La Comisión Europea está elaborando directrices para facilitar la aplicación del Reglamento.

Por último, cabe recordar que en España fue aprobado el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial mediante Real Decreto 729/2023, de 22 de agosto. Esta Agencia ejercerá, entre otras muchas competencias, el fomento de entornos reales de prueba de los sistemas de inteligencia artificial, para reforzar la protección de los usuarios y evitar sesgos discriminatorios, que permitan una correcta adaptación de los sistemas innovadores de inteligencia artificial a los marcos jurídicos en vigor, así como el apoyo al desarrollo y uso de sistemas de IA.

4.-Las estrategias de transformación digital en el sector publico

En España muchas Administraciones Públicas disponen de estrategias de transformación digital para facilitar y promover el desarrollo y la expansión de la IA.

En el ámbito estatal, la Estrategia de Inteligencia Artificial 2024 que se estructura en torno a tres elementos: el primero *es la necesidad de dotar al país de las capacidades necesarias para hacer frente a una demanda creciente de productos y servicios de IA.* El segundo elemento es el impulso a la adopción de IA, con especial foco en su aplicación al sector público y a las empresas pequeñas y medianas (pymes), dado que son las que más apoyo necesitan para abordar esta transformación. El sector público debe, asimismo, ser un impulsor en la adopción de IA, no sólo porque ello supone mejorar la prestación de servicios a los ciudadanos, sino porque además servirá como catalizador y ejemplo para los avances en el sector privado. El tercer elemento fundamental *tiene que ver con la necesidad de alcanzar un amplio consenso sobre los usos de la IA.*

En el ámbito autonómico son numerosas las Comunidades Autónomas que disponen de su estrategia de IA.

La Comunidad de Madrid tiene una Oficina Técnica de Impulso de la Inteligencia Artificial en la Administración con la *finalidad de centralizar los procesos de impulso, estudio, análisis y potenciación relacionados con la inteligencia artificial. Su objetivo es ayudar a definir la estrategia de inteligencia artificial, establecer las mejores prácticas y una sólida gobernanza en toda la administración, reduciendo los riesgos asociados con la dispersión de estos procesos entre distintos equipos.*

En nuestro ámbito local, el Ayuntamiento de Madrid cuenta con una Estrategia de Transformación Digital, situando la IA en el centro*, como palanca facilitadora, impulsando el cambio de modelo de la ciudad, en la mejora de la prestación de servicios digitales y en la atracción de talento, inversión e innovación.* Esta estrategia da una especial relevancia a la ética y la protección de datos digitales. Partiendo del potencial que tiene la IA de influir en distintos ámbitos para *mejorar la vida de la ciudadanía,* e inspirándose en modelos exitosos de la Unión Europea para *asegurar que las nuevas oportunidades que brinda la Inteligencia Artificial*

sean aprovechadas. El documento recoge los avances de la IA en el Ayuntamiento de Madrid, sus objetivos y líneas de actuación. La apuesta por la IA como herramienta para la mejora de los servicios se completa con el compromiso de una implementación correcta, asegurando que sea adecuada y ética.

5.-El uso de la IA en la prevención y detección de prácticas de fraude y corrupción

Es incuestionable la utilidad que los sistemas de IA pueden tener en la prevención y detección de conductas irregulares, de fraude o corrupción. Se podrán manejar y rentabilizar grandes cantidades de datos que permitirán sacar a la luz prácticas no deseables en dicho ámbito. Su mera existencia potencialmente se puede percibir subjetivamente como una mayor capacidad de control y conocimiento de comportamientos en los que existe riesgo de fraude, conflictos de interés, corrupción o irregularidades administrativas, con lo que su existencia por sí misma pudiera ya contribuir a disuadir de dichos comportamientos.

Los sistemas automatizados y los sistemas IA contienen una innegable potencialidad para garantizar el cumplimiento de las leyes evitando o detectando riesgos de vulneración que conduzcan a praxis contrarias a una buena administración. Suponen la utilización de ingentes cantidades de datos, y en este sentido permitirán detectar, con más facilidad y menos recursos humanos, posibles irregularidades.

La utilización de herramientas de la IA para prevenir y atajar comportamientos de fraude, corrupción, conflictos de intereses o irregularidades administrativas tiene un reverso, y es que además de las posibles vulneraciones de derechos por el propio uso incorrecto de algoritmos y datos, también puede ser utilizada precisamente para llevar a cabo dichos comportamientos irregulares.

Al analizar la posible utilización de la IA en materia de prevención y detección de los citados comportamientos, han de tenerse en cuenta tanto los aspectos favorables para la integridad del sector público como los posibles riesgos. Las oportunidades que nos brinda la IA van acompañadas de inevitables riesgos. Estos riesgos no deberían impedir que se usen sistemas de IA para mejorar la integridad del sector público, pero no deben ser ignorados a fin de poder minimizarse o eliminarse.

Hay distintos principios a tener en cuenta por las administraciones públicas:

Transparencia

La exigencia legislativa de transparencia de la actividad de las administraciones públicas y de sus empleados es un medio preventivo de fraude y corrupción. Los datos que han de publicarse deben ser fácilmente accesibles, en formatos reutilizables, veraces y estar actualizados. Estos requisitos son determinantes no solo para el cumplimiento de la obligación legal sino también para su aprovechamiento. Los sistemas IA manejan datos mediante algoritmos, el diseño de estos últimos y la calidad de los datos va a determinar que sean eficaces en la lucha contra la corrupción y, por supuesto, con las debidas garantías a derechos fundamentales. Los datos y algoritmos han de ser transparentes y conocidos por los ciudadanos. Cuestión diferente es la capacidad o formación que éstos tengan para comprenderlos.
El Reglamento IA establece la obligación de transparencia, así su Considerando 27 señala: *que los sistemas de IA se desarrollan y utilizan de un modo que permitan una trazabilidad y explicabilidad adecuadas, y que, al mismo tiempo, haga que las*

personas sean conscientes de que se comunican o interactúan con un sistema de IA e informen debidamente a los responsables del despliegue acerca de las capacidades y limitaciones de dicho sistema de IA y a las personas afectadas acerca de sus derechos. De manera expresa en los sistemas de alto riesgo, el artículo 13 establece la obligación de ser diseñados y desarrollados de modo que se garantice que funcionan con un nivel suficiente de transparencia *para que los responsables del despliegue interpreten y usen correctamente sus resultados de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el proveedor y el responsable del despliegue cumplan las obligaciones pertinentes previstas en la sección 3.*
Las obligaciones con relación a la transparencia de determinados sistemas IA quedan detalladas en al artículo 50 del Reglamento.

Prevención de sesgos y discriminaciones

El Reglamento contiene numerosas referencias a la obligación de que los sistemas IA eviten los efectos discriminatoritos y los sesgos injustos prohibidos por el Derecho nacional o de la Unión.
Los datos que se utilicen y el diseño de algoritmos pueden producir sesgos que induzcan a un análisis erróneo que mediatice a los responsables que han de tomar decisiones en materia de prevención y lucha contra la corrupción, tanto en la inspección de asuntos como en la toma de decisión final. De ahí la importancia de que los datos sean veraces y completos, y sin perjuicio de que tanto en su obtención como manejo se hayan respetado todos los derechos fundamentales. El principio de transparencia de los sistemas contribuye a que puedan llevarse a cabo actuaciones de prevención e inspección ajustadas a criterios no sesgados o discriminatorios, entre otros.
La necesaria supervisión y control sobre los sistemas y sus conclusiones por parte de responsables en la materia es también incuestionable.
Actualmente, en la fase de desarrollo e implantación de los sistemas IA podría considerarse prudente que dichos sistemas sirvieran de apoyo a la toma de decisiones en la lucha contra el fraude y la corrección, pero que no impliquen una sustitución humana total.

Protección de datos

Los datos de alta calidad desempeñan un papel esencial a la hora de proporcionar la estructura de los sistemas de IA y garantizar su funcionamiento. Además, ciertos datos han de estar especialmente protegidos a fin de evitar repercusiones negativas a derechos fundamentales. El Reglamento IA reconoce los múltiples beneficios de la IA, pero también su posibilidad de utilizarse indebidamente y de proporcionar herramientas de manipulación. Estas prácticas han de estar prohibidas pues van en contra de derechos fundamentales, entre otros, a la protección de datos.
El Considerando 69 del Reglamento, señala que: *El derecho a la intimidad y a la protección de datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. A este respecto, los principios de minimización de datos y de protección de datos desde el diseño y por defecto, establecidos en el Derecho de la Unión en materia de protección de datos, son aplicables cuando se tratan datos personales. Las medidas adoptadas por los proveedores para garantizar el cumplimiento de estos principios podrán incluir no solo la anonimización y el cifrado, sino también el uso de una tecnología que permita llevar los algoritmos a los datos y el entrenamiento de los sistemas de IA sin que sea necesaria la transmisión entre las partes ni la copia de los datos brutos o estructurados, sin perjuicio de los requisitos en materia de gobernanza de datos establecidos en el presente Reglamento.*

Por lo que respecta a la lucha contra el fraude y la corrupción no podemos olvidar el contenido de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. La finalidad de esta Ley es "otorgar una protección adecuada frente a las represalias que puedan sufrir las personas físicas que informen sobre alguna de las acciones u omisiones a que se refiere el artículo 2, a través de los procedimientos previstos en la misma".
La protección de datos de las personas informantes de infracciones en el ámbito de la ley es un pilar esencial en la lucha contra el fraude y la corrupción, aspecto que debe tratarse con especial cautela y garantía en el empleo de cualquier herramienta tecnológica antes, durante y después de la investigación. Derecho de protección que también se extiende a las personas afectadas por la información.

Debida motivación de los actos administrativos:

Las herramientas tecnológicas, y en concreto los sistemas de IA en la detección y gestión de actuaciones contrarias al ordenamiento jurídico en materia de fraude y corrupción en el sector público son de gran utilidad, siempre recordando que la Administración Pública debe tramitar sus procedimientos conforme al marco legalmente previsto en las normas que regulan su actuación.
En el ejercicio de las funciones que le son propias, las Administraciones Públicas llevan a cabo actos reglados en los que su actuación está predetermina por la ley de manera precisa, por lo que el margen de decisión es inexistente o muy limitado. En estos supuestos será más fácil la utilización de sistemas automatizados.
Sin embargo, en las actuaciones de carácter discrecional legalmente previstas, donde el órgano competente tiene un mayor margen de decisión, será más cuestionable la posibilidad de sistemas IA más allá de las labores de apoyo. La denominada "reserva de humanidad" quedaría afecta a este tipo de actos, al menos de momento. No obstante, es asunto que está sujeto a muchos debates legales y doctrinales.
En procesos tan complejos como los que se tramitan en materia de fraude, corrupción o comportamientos irregulares, la debida seguridad jurídica de las actuaciones administrativas y las normas vigentes del derecho administrativo nos aleja actualmente de la plena implantación de sistemas de IA y que en su totalidad tramiten y adopten decisiones. Aunque sin duda el apoyo en los medios tecnológicos y los sistemas IA será muy útiles en dichos procesos.
Por último, puede ser oportuno citar la necesaria intervención humana en la toma de decisiones judiciales donde la IA puede servir de ayuda pero no decisoria, como se razona en el Considerando 61 del Reglamento IA, en el que se dice:
Deben clasificarse como de alto riesgo determinados sistemas de IA destinados a la administración de justicia y los procesos democráticos, dado que pueden tener efectos potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales y el derecho a la tutela judicial efectiva y a un juez imparcial. En particular, a fin de hacer frente al riesgo de posibles sesgos, errores y opacidades, procede clasificar como de alto riesgo aquellos sistemas de IA destinados a ser utilizados por una autoridad judicial o en su nombre para ayudar a las autoridades judiciales a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos. También deben considerarse de alto riesgo los sistemas de IA destinados a ser utilizados por los organismos de resolución alternativa de litigios con esos fines, cuando los resultados de los procedimientos de resolución alternativa de litigios surtan efectos jurídicos para las partes. La utilización de herramientas de IA puede apoyar el poder de decisión de los jueces o la independencia judicial, pero no debe substituirlas: la toma de decisiones finales debe seguir siendo una actividad humana. No obstante, la clasificación de los sistemas de IA como de alto riesgo no debe hacerse extensiva a los sistemas de IA destinados a actividades administrativas meramente accesorias que no afectan a la

administración de justicia propiamente dicha en casos concretos, como la anonimización o seudonimización de resoluciones judiciales, documentos o datos, la comunicación entre los miembros del personal o las tareas administrativas.

Códigos de conducta

El Considerando 20 del Reglamento señala que l*a Comisión y los Estados miembros deben facilitar la elaboración de códigos de conducta voluntarios para promover la alfabetización en materia de IA entre las personas que se ocupan del desarrollo, el manejo y el uso de la IA*
Está previsto en el Reglamento que la Oficina de IA y los Estados miembros fomenten y faciliten la creación de códigos de conducta a los proveedores de sistemas de IA que no son de alto riesgo, códigos de conducta destinados a impulsar la aplicación voluntaria de la totalidad o parte de los requisitos aplicables a los sistemas de IA de alto riesgo. Regulado con mayor detalle en el Capítulo X bajo el epígrafe *Código de Conducta y Directrices.*
Actualmente la Comisión Europea está tramitando un Código de Buenas Prácticas para inteligencia artificial de uso general, con participación de variedad de partes involucradas: proveedores de modelos de IA de uso general, proveedores intermedios, organizaciones del sector, sociedad civil, titulares de derechos, representantes del mundo académico y expertos independientes.
Por otra parte, los códigos éticos y planes de integridad, tan importantes en la lucha contra el fraude y la corrupción, pueden contribuir a un desarrollo más ético y transparente de los sistemas IA, con soluciones de consenso unánimemente aceptadas.

6.-Modelos existentes

En la lucha contra el fraude y la corrupción del sector público son diversos los ámbitos donde los sistemas IA tienen potenciales posibilidades de apoyo y desarrollo. Pueden ser utilizados en el control y detección de prácticas irregulares en la contratación pública, en subvenciones, en conflictos de intereses, o comprobación de falsedad de datos o fraudes, entre otros.

Existen ya diversos ejemplos de utilización de herramientas tecnológicas e IA en la lucha contra el fraude y la corrupción en el sector público:

ARACHNE:

Es una herramienta informática de evaluación del riesgo desarrollada por la Comisión Europea mediante la que se pueden identificar de forma efectiva y eficaz los proyectos, contratos, contratistas y beneficiarios de mayor riesgo, que resulta de gran utilidad para verificar que la gestión de Fondos europeos se realiza de conformidad con las disposiciones de aplicación. Se suministra de manera gratuita a las autoridades que gestionan los fondos.
Las autoridades de gestión cuando utilizan el software Arachne deben cumplir las normas nacionales y europeas de protección de datos.
Esta herramienta de evaluación del riesgo alerta a la autoridad de gestión sobre los proyectos, contratos, contratistas y beneficiarios de mayor riesgo, y la ayuda a concentrarse en su capacidad administrativa para las verificaciones.
Se trata pues de una herramienta de análisis que contribuye a mejorar la gestión de los proyectos, no supone una toma de decisiones autónomas. Puede servir para proporcionar datos de calidad a posibles sistemas IA.

DIGIWHIST (denunciante digital):

Es un proyecto de *big data* financiado por la Unión Europea para fortalecer el papel de la sociedad en la lucha contra el fraude y la corrupción en la contratación pública. Sus principales objetivos son mejorar la confianza en los gobiernos y la eficiencia del gasto público dotando a la sociedad civil, a los periodistas de investigación y a los funcionarios públicos, en toda la UE y en algunos países vecinos, de la información y las herramientas que necesitan para aumentar la transparencia del gasto público.
El proyecto recopila y evalúa datos a nivel microeconómico utilizando información procedente de transacciones de contratación pública individuales y de las estructuras financieras y de propiedad de las empresas adjudicatarias. Estos datos se vinculan a información sobre las declaraciones de activos e ingresos con el fin de detectar posibles conflictos de intereses en el sistema de contratación pública y, más concretamente, para identificar vulnerabilidades sistémicas en las respectivas legislaciones y su aplicación.
Es una herramienta de libre acceso para el público.

En España también hay ejemplos de herramientas para la lucha contra el fraude y la corrupción:

MINERVA:

Es una herramienta informática de *datamining* para el análisis de riesgo de conflicto de interés que la Agencia Estatal de Administración Tributaria (AEAT) pone a disposición de todas las entidades decisoras, entidades ejecutoras y entidades instrumentales participantes en el Plan de Recuperación, Transformación y Resiliencia (PRTR), así como de todos aquellos al servicio de entidades públicas que participen en la ejecución del PRTR y de los órganos de control competentes del Mecanismo de Recuperación y Resiliencia (MRR).
Los usuarios de la herramienta habrán de estar previamente autorizados en la aplicación Coffe.
El informe del análisis de riesgos de conflictos de interés contiene información relativa a potenciales beneficiarios para los que se ha detectado existencia de riesgo (bandera roja) y listado de potenciales beneficiarios con ausencia de información de titularidades o personas fallecidas (bandera negra). No se incluirán explícitamente beneficiarios para las que no se ha detectado existencia de riesgo (bandera verde). Para un mismo potencial beneficiario se pueden activar simultáneamente una bandera negra y una o varias banderas rojas (detección de existencia de riesgo por motivos distintos a las titularidades reales).
El informe contiene información detallada de todos los riesgos de conflicto de interés que se habían activado y que han dado lugar a la bandera roja. No muestra la identificación de terceras personas intermedias, sino únicamente una descripción de los riesgos.

BRAVA (*Bid Rigging Algorithm for Vigilance in Antitrust*)

Es una herramienta basada en IA para la detección de la manipulación de licitaciones públicas, que clasifica las ofertas presentadas por las empresas a una licitación como potencialmente colusorias o anticompetitivas.
Su algoritmo, basado en el aprendizaje automático *(machine learning*), toma como fuente la base de datos de contratación pública. Facilita que las autoridades de competencia gestionen toda la información y datos de forma eficiente.

La Oficina Independiente de Regulación y Supervisión de la Contratación Pública (OIReScon) recomienda en su último informe anual, 2024, la "implantación generalizada del uso de herramientas de IA como instrumento de ayuda en la detección de prácticas anticompetitivas y colusorias en la contratación pública". Y destaca a BRAVA como ejemplo.

Sistema de Alertas Tempranas (SALER) Generalitat Valenciana

Este Sistema está regulado en la Ley 22/2018, de 6 de noviembre, de Inspección General de Servicios y del sistema de alertas para la prevención de malas prácticas en la Administración de la Generalitat y su sector público instrumental.
El sistema está descrito en el artículo 17 de la ley en los siguientes términos: *El sistema de alertas se articulará a través de un conjunto de herramientas cuya interacción permite la detección de posibles irregularidades y malas prácticas administrativas, con carácter preventivo, a partir del análisis de la información obtenida y de la evaluación de factores de riesgo que potencialmente pudieran originarlas.*
Está constituido por el conjunto de herramientas de software y la infraestructura de servidores y bases de datos. *Los datos pueden proceder de tres fuentes: bases de datos internas creadas y mantenidas por la administración de la Generalitat y su sector público instrumental con los datos que los interesados han proporcionado voluntariamente para la tramitación del procedimiento a través del cual se han relacionado con la administración; bases de datos de organismos o entidades externas con los que se establezca una colaboración, por ejemplo registros públicos; y, finalmente, datos de carácter personal que sus titulares hayan hecho manifiestamente públicos, particularmente en internet* (Preámbulo).
El uso de algoritmos informáticos permite analizar automáticamente la gran cantidad de datos e información reduciendo la carga de trabajo de los órganos de control. Son estos los que adoptan las decisiones, no el sistema.

ISSA *(Inteligencia Artificial+Seguridad Social):*

Desde 2020 la Seguridad Social tiene su propio asistente virtual (CHATBOT) para proporcionar información útil y orientar a los ciudadanos sobre los servicios más demandados de la Seguridad Social. Permite mantener conversaciones y ofrecer respuestas con información oficial y de confianza en materia de Seguridad Social.
Esta plataforma incorpora técnicas de Inteligencia Artificial y de aprendizaje automático para que la mejora continua del asistente le permita adaptarse a las necesidades y preguntas de los ciudadanos

7.-Conclusiones

La utilización de sistemas IA en la lucha contra conductas de fraude y corrupción en el sector público está cada vez más presente, tanto en la prevención como en la detección y gestión de dichas conductas.

El análisis e investigación de posibles comportamientos irregulares vinculados a dichas cuestiones presentan una sensibilidad y complejidad singulares, dado que las consecuencias de esos comportamientos pueden ser administrativas pero también penales.

La prudencia, el equilibrio y la proporcionalidad han de regir las decisiones jurídico-tecnológicas de utilización y desarrollo de los sistemas IA, teniendo en cuenta que presentan indudables ventajas pero también riesgos.

Cuestión de gran importancia será la elección de algoritmos adecuados a la naturaleza de esta materia, así como la garantía de que los datos a utilizar sean rigurosos, solventes y de alta calidad. En estos casos conviene que los datos procedan de fuentes oficiales, bien del ámbito interno de la Administración de que se trate, bien de otras Administraciones, entidades u organizaciones públicas que den garantía de la calidad de los datos, para lo cual podrán suscribirse convenios de colaboración en los marcos legalmente establecidos, siempre con el cumplimiento de los requisitos de transparencia y protección de datos.

En el ámbito local serán diferentes los campos de lucha contra el fraude en los que puedan utilizarse los sistemas IA, desde la contratación pública, pasando por las subvenciones, el urbanismo o el conflicto de intereses. No obstante, en numerosas ocasiones será necesario firmar convenios para poder utilizar bases de datos de otras administraciones públicas, donde reside mucha de la información necesaria.

Es de gran importancia la debida formación educativa y profesional de los empleados públicos, tanto en el desarrollo como en la utilización de los sistemas. Y sin olvidar el carácter esencial de las estrategias en materia de IA, ya existentes en varias administraciones locales, como es el caso de la Ciudad de Madrid, que permitirá su desarrollo en un entorno innovador, seguro y ético.

Actualmente los sistemas IA se configuran como sistemas idóneos para la lucha contra el fraude y la corrupción en su vertiente de apoyo y complementariedad en las distintas fases de la investigación, bien para permitir atisbar situaciones que deban ser analizadas bien para comprobar la existencia de las irregularidades, pero en todo caso la decisión última en la adopción de las resoluciones tendrá que ser humana.

Casa de Cisneros - Plaza de la Villa, 4 - 28005 MADRID
T.: +34 915 887 531 – 914 802 604
oficinacontrafraude@madrid.es