



Working Papers  
2025, 1(5):58-70, © DIGITAPIA  
Universitat Oberta de Catalunya  
<https://blogs.uoc.edu/digitapia/>

DIGITAPIA

## La automatización del control administrativo

### *The automatization of the administrative control*

Oscar Capdeferro Villagrasa<sup>1</sup>

Profesor Agregado de Derecho Administrativo, Universidad de Barcelona

[ocapdeferro@ub.edu](mailto:ocapdeferro@ub.edu)

#### Resumen

La administración está adaptando sus medios y técnicas de control a la tecnología disponible, mediante la incorporación de herramientas de detección de infracciones cada vez más sofisticadas y autónomas. Sin embargo, esta reforma en los medios de comprobación, inspección y sanción, conlleva algunas cuestiones problemáticas que pueden abordarse mediante una reforma normativa, como la falta de transparencia, o la falta de previsión sobre cómo gestionar los resultados del sistema algorítmico en consideración a situaciones de falso positivo o falso negativo.

**Palabras clave:** Control, Inspección, Procedimiento sancionador, Actuación administrativa automatizada.

#### Abstract

The administration is adapting its control methods and techniques to the available technology by incorporating increasingly sophisticated and autonomous tools for detecting violations. However, this transformation in verification, inspection, and sanctioning mechanisms raises certain challenges that may require regulatory reform. Issues such as lack of transparency and the absence of clear guidelines on handling algorithmic system outcomes—particularly in cases of false positives or false negatives—must be addressed to ensure fairness and accountability.

**Keywords:** Control, Inspection, Sanctioning procedure, Automated administrative action.

---

<sup>1</sup>Oscar Capdeferro Villagrasa, Profesor Agregado de Derecho Administrativo de la Universitat de Barcelona (UB), es licenciado en Derecho (UB, 2009), Máster Avanzado en Ciencias Jurídicas (UPF, 2010) y doctor en Derecho (UB, 2015), con Mención Internacional y Premio Extraordinario de Doctorado del curso 2014-2015. Ha realizado estancias de investigación en las siguientes universidades extranjeras: Università di Bologna, en la Università degli Studi di Ferrara, en la Università di Roma LUMSA y en la University of Oxford. Su producción científica se ha centrado principalmente en el estudio de la corrupción pública, materia en la que destaca la monografía «El derecho administrativo y la prevención de la corrupción urbanística» (Marcial Pons, 2016), Premio Jurídico Ferrer Eguizábal 2015 en Derecho administrativo; así como en los efectos que puede conllevar el uso de la inteligencia artificial en la mejora del servicio público, sobre lo que también ha escrito capítulos de libro y artículos científicos.

# 1 Introducción

En la actualidad, se emplean herramientas digitales que automatizan, en mayor o menor medida, los controles de cumplimiento del ordenamiento jurídico llevados a cabo por la administración pública. Estos controles pueden llevarse a cabo de forma completamente automatizada, como sucede con los sistemas que, a través de los dispositivos correspondientes (como cámaras o radares), detectan automáticamente una infracción de tráfico y, sin intervención humana, procesan y emiten la denuncia correspondiente<sup>2</sup>. O bien pueden contar con un grado de automatización menor que no excluye la participación humana, lo que se ha denominado semiautomatización<sup>3</sup>, tal y como sucede, por ejemplo, cuando la administración hace uso de sistemas digitales que se limitan únicamente a alertar al equipo inspector humano correspondiente de eventuales indicios de infracción o de situaciones anómalas, para que el inspector o inspectora competente lleve a cabo, con posterioridad, las tareas de comprobación e investigación tendentes a identificar y constatar los posibles incumplimientos del ordenamiento jurídico y las infracciones asociadas a tales incumplimientos.

Este avance en la modernización de los medios de la Administración pública para efectuar sus actuaciones de control se extiende a funciones y ámbitos muy variados, aunque puede destacarse la lucha contra el fraude y la corrupción como un espacio especialmente destacado en el uso de sistemas digitales para procesar datos y detectar irregularidades<sup>4</sup>, generalmente a través de sistemas de alerta, o de banderas rojas (*red flags*).

En el presente capítulo se exponen, en primer lugar y brevemente, algunos de los avances regulatorios en materia de automatización de controles, junto con una exposición de algunas problemáticas destacadas que se han suscitado en relación con los sistemas automatizados o semiautomatizados de control. A continuación, se dedica una sección a presentar algunas experiencias prácticas de sistemas digitales empleados

por las administraciones públicas en sus actuaciones de control. Por último, a la luz de la discusión inicial de problemáticas, y teniendo en cuenta el estado actual y capacidades de los sistemas presentados, se formula y justifica una propuesta regulatoria para los sistemas digitales que automatizan tareas administrativas de inspección y control.

## 2 Estado de la cuestión: avances regulatorios y aspectos problemáticos

El primer problema que surge con el uso de sistemas algorítmicos en las actuaciones de control es que estos sistemas tienden a caer en la informalidad, en el sentido de que su aprobación y puesta en funcionamiento no está cubierta explícitamente por una norma jurídica, y su uso, al menos en los casos de controles que cuentan con un grado de automatización menor (semiautomatizados), se puede calificar como actuación previa (art. 55 Ley 39/2015)<sup>5</sup>, fuera de la actuación formalizada del procedimiento administrativo inspector, o sancionador, que corresponda.

Este punto ha sido corregido en algunas, pocas, prácticas que se pueden destacar. En primer lugar, el antecedente de la Ley valenciana 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, ha marcado una línea poco seguida: la aprobación del uso del sistema digital de control mediante ley. Esta experiencia puede ser calificada como una buena práctica, en mi opinión, por las opciones regulatorias que ofrece el rango de ley. Entre los principales aspectos a considerar, la aprobación por ley dota al regulador con mayor capacidad para determinar el empleo de datos tratados por el sistema y, sobre todo, permite introducir infracciones y sanciones vinculadas con el uso del sistema<sup>6</sup>.

En segundo lugar, se puede destacar el sistema Minerva, cuyo uso fue aprobado por la orden ministe-

<sup>2</sup>Véase [Martínez Otero \(2024\)](#), p. 5.

<sup>3</sup>En esta línea, algunos autores se han referido a las decisiones semiautomatizadas ([Ponce Solé, 2024](#), p. 178); y ([Martín Delgado, 2023](#), p. 161); y a la actuación administrativa semiautomatizada ([Mir Puigpelat, 2023](#), p. 8). Es este también el planteamiento de la Carta de Derechos Digitales, cuando reconoce que «Será necesaria una evaluación de impacto en los derechos digitales en el diseño de los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas» (Carta de Derechos Digitales, XVI, 7).

<sup>4</sup>Véanse [Ranchordás and Schuurmans \(2020\)](#), p. 6; y [Poltoratskaia and Fazekas \(2024\)](#).

<sup>5</sup>Véase [Miranzo Díaz \(2023\)](#), p. 112. En el mismo sentido, consultar [Ponce Solé \(2019\)](#). Me he referido asimismo a esta cuestión, con mayor detalle, en [Capdeferro Villagrasa \(2019\)](#), p. 19.

<sup>6</sup>Así lo establece el principio de legalidad de la potestad sancionadora (art. 25 Ley 40/2015) y art. 25 CE. Entre otras, se puede destacar la STC 61/1990, de 29 de marzo, en la que se declara la nulidad de las sanciones impuestas en aplicación de un precepto de la orden ministerial reguladora de la profesión de detective privado, también declarado nulo por el Tribunal Constitucional, por ser contrarios al art. 25.1 CE debido al rango de la norma, y también por aspectos sustantivos.

rial HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia (PRTR). En este caso, el instrumento regulador empleado permite fijar elementos procedimentales que acompañan al uso del sistema, diseñando un sistema de procedimiento de gestión de banderas rojas que se impone a las administraciones en el uso de fondos del PRTR. Otro elemento para destacar de la regulación del sistema Minerva es, hasta cierto punto, el grado de explicación que da la propia norma sobre el funcionamiento del sistema. Así, se indican las principales fuentes de información que emplea y cruza<sup>7</sup>, así como la tarea que realiza el sistema<sup>8</sup> y la finalidad perseguida con esa acción, consistente en analizar «las posibles relaciones familiares o vinculaciones societarias, directas o indirectas, en las que pueda haber un interés personal o económico susceptible de provocar un conflicto de interés», (art. 3.3 de la misma orden).

Relacionado con el problema anterior de cobertura normativa, otro punto problemático que merece consideración es que, a fin de poder emplear un sistema algorítmico como base para iniciar actuaciones de investigación, es necesario que se pueda justificar tal habilitación en el ordenamiento jurídico, en tanto que la administración actúa con sometimiento pleno a la ley y al Derecho (art. 103 Constitución Española).

Esta cuestión se presenta como una problemática entre los organismos o instituciones con facultades de control cuando quieren poner en funcionamiento herramientas para detectar, indiciariamente, posibles irregularidades que investigar, ya que es posible que su normativa reguladora no permita investigar hechos de oficio, sin una previa denuncia.

Este matiz puede ser relevante, por ejemplo, en el momento actual, en que las agencias autonómicas anticorrupción están desarrollando, o preparando el desarrollo, de sistemas algorítmicos de alertas de posibles casos de corrupción. Así, la Ley 11/2016, de 28 de noviembre, de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana, en su art. 11.1 permite iniciar las investigaciones de casos de corrupción o fraude de oficio también «cuando, después de realizar un análisis de riesgo, los indicadores de riesgo aconsejen la inspección o el seguimiento de determinados hechos o actividades». En términos similares se regulaba la iniciativa en las actuaciones de investigación en el art. 14.1.a de la derogada Ley 16/2016, de 9 de diciembre, de creación de la Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears<sup>9</sup>. Frente a esta explícita cláusula que podría amparar el uso de sistemas de alertas, en la legislación de las demás oficinas parece más abierto y menos claro si el uso de estos sistemas pueda contar con una base suficiente para iniciar investigaciones. Así, en las demás leyes se suele hacer una referencia básica a que la dirección de la oficina puede iniciar, de oficio, a iniciativa propia, las actuaciones de investigación<sup>10</sup>. Además, se añade, en el caso andaluz, un listado abierto de circunstancias de las que puede traer causa el inicio por iniciativa propia, en el que, aunque si bien es cierto que no se hace referencia a sistemas digitales de alertas o indicadores de riesgo, se alude a cualquier otro medio válido en derecho<sup>11</sup>.

Otro problema que se debe tener en cuenta es que los sistemas algorítmicos pueden generar resultados erróneos, marcando falsos positivos o falsos negativos<sup>12</sup>. Un falso positivo puede derivar en sanciones injustificadas, mientras que un falso negativo puede permitir que conductas ilícitas pasen desapercibidas.

<sup>7</sup>Se trata, en este caso, de la información de la propia persona implicada en el caso a través de la consignación de la correspondiente declaración de ausencia de conflicto de interés, y los datos que obran en la Agencia Tributaria, de acuerdo con el apartado 4 de la disposición adicional centésima décima segunda de la Ley 31/2022, de 23 de diciembre, de Presupuestos Generales del Estado para 2023.

<sup>8</sup>«Una vez realizado el cruce de datos, MINERVA ofrecerá el resultado del análisis de riesgo de conflicto de interés al responsable de la operación, al día siguiente, con tres posibles resultados, cuyo significado y efectos son [...]» (art. 5 Orden HFP/55/2023).

<sup>9</sup>Cabe destacar que, de forma polémica, esta oficina antifraude fue suprimida, con la derogación de su ley de creación, con efectos de 19 de abril de 2024, por la disposición derogatoria única.1 de la Ley 2/2024, de 11 de abril, de creación del Registro de Transparencia y Control del Patrimonio y de las Actividades de los Cargos Públicos de las Illes Balears.

<sup>10</sup>Ver art. 14.1 Ley Foral 7/2018, de 17 de mayo, de creación de la Oficina de Buenas Prácticas y Anticorrupción de la Comunidad Foral de Navarra; art. 20.a Ley 2/2021, de 18 de junio, de lucha contra el fraude y la corrupción en Andalucía y protección de la persona denunciante; art. Ley 14/2008, de 5 de noviembre, de la Oficina Antifraude de Cataluña y art. 16 de las Normas de actuación y de régimen interior de la Oficina Antifraude de Cataluña, aprobadas por la Comisión de Asuntos Institucionales en su sesión del día 25 de noviembre de 2009.

<sup>11</sup>Se establece lo siguiente: «A iniciativa propia, cuando, a la vista de los informes de la Cámara de Cuentas de Andalucía, del Tribunal de Cuentas, de la Inspección General de Servicios, de la Intervención General de la Junta de Andalucía o por cualquier otro medio válido en derecho, la Oficina tuviera conocimiento de hechos que pudieran ser constitutivos de fraude, corrupción o conflicto de intereses» (art. 20.a Ley 2/2021, de 18 de junio, de lucha contra el fraude y la corrupción en Andalucía y protección de la persona denunciante).

<sup>12</sup>Un falso positivo se da cuando un sistema alerta sobre una circunstancia que no es real. Véase Baader and Krcmar (2018), p. 1. Contrariamente, un falso negativo sería la omisión del sistema en la detección de un indicador o bandera roja.

En particular, resulta problemático el falso positivo para las personas controladas, ya que pueden ser objeto de actuaciones de inspección invasivas, que pueden afectar incluso a derechos fundamentales, como por ejemplo si se realiza una entrada y registro en domicilio, o incluso pueden ser sancionadas de forma injusta, a partir de unos indicios o hechos erróneamente advertidos, o malinterpretados, por el sistema algorítmico. En este punto, un ejemplo que ilustra claramente el error del sistema en la interpretación de la realidad, dando lugar a falsos positivos de forma masiva, se ha dado en el control automatizado de acceso de vehículos en las zonas de bajas emisiones.

En efecto, desde que se puso en funcionamiento en el área metropolitana de Barcelona<sup>13</sup>, el sistema tecnológico de captación de imágenes permitía que un sistema algorítmico controlara las matrículas de los vehículos que accedían, cruzando los datos de las matrículas de los vehículos que identificaba en las imágenes con el listado de vehículos que estaban autorizados para el acceso. Pronto, empezaron a proliferar propuestas injustas de sanciones a titulares de vehículos antiguos y contaminantes que no tenían permitido el acceso a la zona de bajas emisiones, por haber entrado en dicha zona, cuando realmente esos vehículos no habían entrado circulando, sino remolcados por grúas, camino a talleres mecánicos o incluso a desguaces<sup>14</sup>. En esos casos, el problema radicó en que el sistema informático leía las matrículas, pero no interpretaba el contexto de la imagen, de tal modo que, contrariamente a lo dispuesto en la normativa, entendía sancionable el acceso aun en casos en que el vehículo iba remolcado. Durante todo este proceso, desde la captación hasta la emisión de la propuesta de sanción, tal y como quedó constatado por la Sindicatura de Greuges municipal, ninguna persona veía las imágenes captadas<sup>15</sup>, por lo que se estaría ante un control plenamente automatizado en el que, además, sucedían errores que habrían sido evidentes para un controlador humano que hubiera revisado las imágenes. Esta sorprendente situación es declarada por la Sindicatura como contraria al derecho a una buena administración, en tanto que, siguiendo al Tribunal Supremo (en sentencia de 14 de mayo de 2019), se con-

sidera que no hay una conducta suficientemente diligente para evitar las posibles disfunciones derivadas de la actuación administrativa, y se recomienda explorar las soluciones técnicas para poder realizar cribados de imágenes<sup>16</sup>.

Ante este tipo de problemáticas, resulta importante destacar aquellas normas que han previsto garantías o mecanismos ante el falso positivo.

En primer lugar, en 2022 entró en vigor la reforma del Real Decreto 928/1998, de 14 de mayo, por el que se aprueba el Reglamento general sobre procedimientos para la imposición de sanciones por infracciones de orden social y para los expedientes liquidatorios de cuotas de la Seguridad Social, mediante la cual se introdujo en el ámbito de las inspecciones y sanciones en materia laboral una regulación específica para la actuación automatizada de control de la Inspección de Trabajo y Seguridad Social<sup>17</sup>. Dicha regulación prevé la posibilidad de generar de forma automatizada actas de infracción, e incluso las propuestas de resolución (art. 44).

Como elemento garantista en este ámbito, y que podría ser efectivo para minimizar los efectos perjudiciales de los falsos positivos sobre los sujetos controlados, se prevé que en caso de que haya alegaciones a las actas de infracción, éstas deberán ser revisadas por el personal inspector (art. 47.3), y, además, en caso de que se hayan formulado alegaciones a las actas de infracción, ya no será posible la elaboración automatizada de propuestas de resolución del procedimiento sancionador (art. 44.1).

Otra previsión de garantía importante es que se impone en el art. 45 que, entre otros extremos, las actas de infracción elaboradas de forma automatizada deberán indicar de forma expresa que se trata de una actuación administrativa automatizada, y se deberá indicar también cuáles han sido los medios utilizados para la comprobación de los hechos que fundamentan el acta. Se trata, pues, de información que posteriormente puede facilitar la formulación de las alegaciones correspondientes de la persona interesada que pueda haberse visto afectada por un falso positivo, derivado de un error del sistema.

<sup>13</sup>AMB (2021).

<sup>14</sup>Han sido relativamente frecuentes las noticias sobre esta problemática, desde 2020 hasta 2024. Por todas, pueden consultarse dos noticias en: *Metropoli*, «Continúan las multas de la ZBE a vehículos arrastrados por grúas»; y *El País*, «Barcelona multa a un coche que circulaba por una ZBE a bordo de una grúa municipal».

<sup>15</sup>Así, la *Resolució de la Sindicatura de Greuges* accesible en: *Síndic de Greuges*, «Queixa relativa al Dret a una bona administració (gestió i recaptació)»

<sup>16</sup>Ibid.

<sup>17</sup>Asimismo, se prevé esta posibilidad en la ley correspondiente, véase el artículo 53.1.a) del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.

Otro buen ejemplo de solución ante posibles falsos positivos se contiene en la Orden HFP/55/2023, en relación con el sistema Minerva, al que ya se ha aludido. En este caso, cuando el sistema algorítmico genera un positivo mediante la señalización de una bandera roja, se prevé que, si la persona afectada por el positivo, señalada por la bandera roja, considera que ese positivo es erróneo, puede optar por no abstenerse y alegar de forma motivada su no reconocimiento de la validez o veracidad del resultado ofrecido por el sistema automatizado de control, lo que da lugar a un procedimiento que deberá resolver el superior jerárquico del decisor público afectado por la bandera roja, por lo que este es, en última instancia, quien se encargará de validar, o descartar, el resultado ofrecido por el sistema Minerva.

Como se ha podido ver, en estos dos ejemplos la normativa prevé explícitamente, creo que con acierto, la opción de poner en cuestión el resultado del sistema algorítmico antes de que sus resultados produzcan efectos, y trasladan a un controlador humano la responsabilidad última de validar, o no, los resultados generados por el sistema algorítmico cuando el resultado inicial del sistema desencadena la formulación de alegaciones por parte de la persona perjudicada por el resultado.

Existe, también, otra forma de acercarse al establecimiento de garantías ante el falso positivo distinta, propia del control semiautomatizado, y que difiere de las dos formas de control automatizado vistas antes, ya que, en caso de controles semiautomatizados, el sistema a menudo interviene en una fase preliminar del control como posible base para iniciar labores de inspección, y, por tanto, no hay ninguna constatación de infracciones que sea comunicada a la persona presuntamente infractora. No hay, pues, espacio para posibles alegaciones, porque no se ha comprobado ni constatado nada todavía, sino que únicamente se ha puesto a disposición del cuerpo inspector el indicio de una posible infracción<sup>18</sup>.

Este es el enfoque que sigue la ley valenciana, 22/2018, reguladora del sistema Saler. En efecto, en dicha ley se prevé que, cuando el sistema digital genere una alerta, el equipo inspector se encargará de calificarla en una de las varias categorías previs-

tas (art. 31). Esta previsión supone, pues, que los resultados del sistema son revisados individualmente por personal inspector humano, y este es el que, en última instancia, determina si procede iniciar alguna actuación de investigación o si debe ignorarse esa alerta. De hecho, una de las categorías en que puede calificarse la alerta es en la de «falso positivo».

Sin embargo, puede criticarse de esta regulación que, aunque menciona expresamente el falso positivo, reduce mucho su definición, al entender que únicamente es falso positivo la alerta infundada que deriva de un error en los datos (art. 31.1.a), dejando de lado posibles errores de programación o de funcionamiento del sistema, falta de actualización de datos, u otras causas que pudieran derivar en una alerta que no esté señalando ninguna situación irregular<sup>19</sup>.

Más allá de la correspondiente cobertura normativa para su uso, también plantea problemas la robustez del resultado que genera el sistema algorítmico. Conviene preguntarse, entonces, pues, si el sistema genera un resultado que pueda hacerse valer como indicio válido para justificar materialmente el inicio de actuaciones de investigación, y, muy especialmente, las actuaciones de investigación más invasivas o perjudiciales sobre derechos fundamentales. Esta cuestión se ha suscitado, especialmente, en los juzgados y tribunales, en relación con las peticiones de entrada y registro en domicilio formuladas por organismos de control, como la Agencia Tributaria o las autoridades de control de la competencia<sup>20</sup>.

Así, el Tribunal Supremo, en su sentencia de 15 de noviembre de 2021<sup>21</sup>, consideró improcedente la entrada en un domicilio, con el objeto de realizar actuaciones de comprobación, en un caso en el que la justificación de la administración tributaria se basaba en «meras conjeturas o inferencias a partir de magnitudes meramente estadísticas -esto es, genéricas», y critica el hecho que el auto recurrido guarde «silencio sobre la seriedad o fiabilidad de tales indicios y la necesidad de la entrada en domicilio como única posibilidad de verificar su acomodo a la realidad» (FD Segundo.6). En este caso, la Agencia Tributaria había solicitado autorización judicial para poder entrar, por sorpresa, sin previo aviso al sujeto inspeccionado (in-audita parte), en el domicilio de una empresa para realizar actividades de comprobación, con la sospecha

<sup>18</sup>En esta línea parece alineada la estrategia de IA de la Agencia Tributaria de mayo de 2024, en la que se afirma que «Las actuaciones administrativas automatizadas que dicte la Agencia Tributaria no descansarán en ningún caso, de manera exclusiva en el resultado obtenido de un sistema de IA. En estas situaciones, se garantiza siempre la intervención humana que habrá de supervisar las decisiones que hayan podido ser propuestas por el sistema, validándolas o modificándolas» (AEAT, 2024, p. 13).

<sup>19</sup>Como ejemplo sobre efectos perjudiciales de falsos positivos, en el ámbito académico, vid. [Giray \(2024\)](#).

<sup>20</sup>Con carácter general, véanse los artículos 18.3 y 100.3 Ley 39/2015.

<sup>21</sup>Roj: STS 3502/2021 - ECLI:ES:TS:2021:3502.

de que podría estarse cometiendo una infracción (por ocultar ventas, no declaradas, por ejemplo), puesto que, al ponerse en relación los datos de facturación de esa empresa con la media nacional en ese sector, se detectaba una rentabilidad excesivamente baja. Cabe añadir que, en este caso, tampoco se había notificado el inicio del procedimiento inspector al sujeto inspeccionado, lo que contradice la jurisprudencia establecida ya en sentencia de 1 de octubre de 2020, y que en esta sentencia el Tribunal Supremo reitera, consistente en que la «autorización judicial de entrada y registro en un domicilio constitucionalmente protegido debe estar conectada con la existencia de un procedimiento inspector ya abierto y cuyo inicio se haya notificado al inspeccionado, con indicación de los impuestos y periodos a que afectan las pesquisas por derivar tal exigencia de los artículos 113 y 142 de la LGT».

Parece, pues, relevante poder garantizar que los sistemas algorítmicos que van a utilizar los cuerpos inspectores empleen unos indicadores de riesgo relevantes y que permitan obtener indicios significativos, y, además, tras la obtención de este primer indicio, se necesitaría de la correcta iniciación, formalizada, de actuaciones de inspección, que permitan concretar más la posible infracción y su alcance, antes de proceder a actuaciones inspectoras de mayor alcance, como es marcadamente la afectación a derechos fundamentales, como en el caso expuesto. En definitiva, la fiabilidad y explicabilidad de los resultados generados por el sistema se presentan como fundamentales, si se utilizan para justificar inspecciones o fundamentar la imposición de sanciones, y debería ser posible garantizar su precisión y validez.

Otro elemento controvertido es la opacidad de los sistemas algorítmicos de control<sup>22</sup>, ya que se ha generalizado la idea que la difusión de información sobre los sistemas empleados en el control sirve a su vez como orientación para que los sujetos infractores puedan eludir el control<sup>23</sup>. Así, puede ser comprensible, hasta cierto punto, la opacidad en el funcionamiento exacto del sistema, especialmente en cuanto a los indicadores de riesgo empleados y los datos específicos que resultan relevantes en ese ámbito, los patrones de compor-

tamiento sospechosos que se buscan, o el índice exacto de variación que hace saltar la alerta.

Sin embargo, en este punto, considero relevante tener en cuenta que el listado de infracciones, obviamente, es público y figura en las leyes y reglamentos ejecutivos correspondientes. Así, las conductas irregulares que puede detectar el sistema, podrían hacerse públicas sin poner en riesgo la efectividad del sistema para detectar posibles infracciones. Incluso, caso por caso, podría valorarse si podría publicarse sucintamente qué indicadores y datos se emplean para lograr la finalidad de detección prevista para el sistema algorítmico, ya que es probable que esa información tampoco suponga desvelar detalles concretos que puedan usarse para eludir el control del algoritmo.

Pensemos, por ejemplo, en el caso en que se hace público que un sistema de la Agencia Tributaria busca posibles casos de fraude tributario a partir del cruce de datos sobre declaraciones de niveles de ingresos y facturación de empresas, y se indica que se ponen esos datos en relación con la media nacional de nivel de facturación e ingresos de empresas similares a fin de detectar casos sospechosos de fraude por bajos niveles declarados. Pues bien, con esa información, una empresa difícilmente va a encontrar referencia alguna para cambiar su forma de actuar fraudulenta para ajustarla al funcionamiento del algoritmo. Sin embargo, quizás podría alterar el comportamiento del posible infractor si la información que se hace pública indica también el índice de referencia del algoritmo y, por ejemplo, se indica públicamente que el sistema detecta aquellas empresas que declaran unos ingresos inferiores al 30% de la media de las empresas similares de la provincia. Así, pues, podría reservarse el índice concreto de la alerta, publicándose la información genérica restante antes indicada, y que en principio no supondría ofrecer indirectamente ninguna orientación específica para eludir el control pretendido.

Un último elemento de transparencia que se podría considerar relevante es el hecho de que se pueda conocer si el sistema algorítmico está alcanzando los resultados previstos, es decir, si su funcionamiento supone realmente una forma eficiente de modernizar

<sup>22</sup>De hecho, incluso puede afirmarse que la opacidad está generalizada y va más allá de las tareas de control: «En el caso del sector público es especialmente preocupante que tan siquiera sepamos qué sistemas de IA existen e impactan en la actuación y prestación de servicios así como en nuestros derechos» (Cotino Hueso, 2023, p. 24).

<sup>23</sup>Así, se ha afirmado que: «if the public knows exactly which things on a tax return are treated as telltale signs of fraud, tax cheats may adjust their behaviour and the signs may lose their predictive value for the agency» (Kroll et al., 2017, p. 658). Y también, en relación con el caso SyRI, de Países Bajos: «the Court found that the legislation provided little, if any, insight into the risk model and risk indicators used, the objective factual data that could justifiably lead to the inference of an increased risk or the data processed in SyRI projects. Crucial information concerning the algorithm's use was deliberately kept secret—an instance of intentional opacity. The Netherlands' refusal to disclose additional information, on the grounds that citizens would otherwise 'game the system', is an argument invoked by many countries with regard to different uses of algorithmic systems in different areas» (Rachovitsa & Johann, 2022, p. 11).

los controles o si más bien ha sido un gasto de recursos económicos que no logra alcanzar los resultados previstos. No es habitual conocer el funcionamiento de estas herramientas, ya que la dinámica habitual en las administraciones españolas es que las memorias de actividad de las instituciones y organismos que disponen de ellas guarden silencio sobre las mismas. Aun así, en ocasiones se puede localizar algún dato o información relevante al respecto, como sucede en el caso de las memorias de la Inspección General de Servicios valenciana, en relación con el sistema Saler. En ellas, se aprecian algunas indicaciones sobre el funcionamiento de Saler, y se desprende que por el momento presenta algunas dificultades para lograr operar de modo efectivo, especialmente por la insuficiencia de datos o por los errores contenidos en los datos<sup>24</sup>.

Para conocer datos sobre el funcionamiento del sistema Minerva, formulé una solicitud de acceso a información a la Agencia Tributaria, en la que pedí la siguiente información:

1. Cuántas banderas rojas ha detectado el sistema Minerva.
2. En los casos de banderas rojas detectadas, en cuántos ha habido abstención de la persona afectada y en cuántos la persona señalada por la bandera roja ha actuado a pesar de la bandera roja detectada.
3. En los casos en que alguien ha actuado en el procedimiento como decisor a pesar de estar afectado por una bandera roja, ¿cuál ha sido el motivo para justificar que no debía abstenerse? (Por ejemplo, datos desactualizados.)
- 4.Cuál es el porcentaje de cada uno de los resultados posibles de Minerva, es decir, qué porcentaje del total de resultados han sido banderas rojas, ausencia de estas, o banderas negras.
5. ¿Qué seguimiento hace la AEAT o la IGAE de las banderas rojas?

La respuesta dada por la administración a esta solicitud, de fecha 31 de julio de 2024, indica lo siguiente: «Teniendo en cuenta la ingente información que hay que analizar y evaluar, correspondiente al envío de peticiones de análisis de conflicto de interés, además de la cantidad de 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), se

concluye que, actualmente la información solicitada no está disponible tal y como usted la solicita, ya que su extracción, es de una gran complejidad técnica y para su aportación sería necesario un proceso previo de reelaboración».

Se añade, también, que: «dado que MINERVA no está diseñada para considerar interacciones entre expedientes o resultados acumulados, ni para realizar extracciones detalladas sobre la actuación de entidades decisoras, entidades ejecutoras o entidades instrumentales, así como la extracción de porcentajes de resultados posibles, la información solicitada no debe explotarse informáticamente de forma directa, tal y como usted solicita, dado que para su aportación sería preciso realizar , con carácter previo, un importante y laborioso proceso previo de reelaboración, haciendo uso de diferentes herramientas de análisis de información, de un alto volumen de resultados de expedientes correspondientes a solicitudes de numerosos y diferentes órganos de contratación de distintas administraciones que se precisa sistematizar, ordenar para evitar duplicidades, y contrastar».

Así, se zanja la cuestión señalando que resulta aplicable la causa de inadmisión del art. 18.1.c de la Ley 19/2013, por necesidad de «una acción previa de reelaboración». Puede ser comprensible que la Agencia Tributaria, responsable y gestora del sistema Minerva, no tenga constancia de información suficiente para contestar detalladamente a la petición número 2 o, sobre todo, la número 3, pero resulta muy curioso, cuanto menos, que no se haya estado en disposición de contestar a la primera y a la cuarta petición de información.

Creo que se debería considerar si es aceptable que en el diseño del sistema algorítmico de control no se haya considerado relevante poder contar con la información agregada o acumulada de funcionamiento del sistema, lo que podría ser un gran indicador de la efectividad de este, a fin de validar su funcionamiento, o para detectar y corregir eventuales insuficiencias o carencias.

### 3 Experiencias. Algunos sistemas de control empleados en España

- Sistema Saler: Se trata del primer sistema algorítmico de control aprobado mediante ley en España, mediante la citada ley valenciana 22/2018, el cual se integra en un innovador sistema de con-

<sup>24</sup>Véase [Generalitat Valenciana \(2022\)](#), pp. 33-35.

trol de malas prácticas administrativas basado en el riesgo. El sistema algorítmico genera alertas sobre malas prácticas, que serán posteriormente analizadas y priorizadas, si procede, para su posterior comprobación o seguimiento por parte del equipo humano encargado de la inspección. La Ley valenciana 22/2018 incorpora también un régimen sancionador para garantizar el correcto uso y funcionamiento del sistema. Entre otros aspectos, también se puede destacar que el sistema prevé emplear, entre otros datos, aquellos que hayan sido hechos manifiestamente públicos en redes sociales, cuando «se trate de páginas indexables por buscadores, espacios abiertos a todos los miembros de la red, redes sociales abiertas o redes cuya naturaleza profesional, empresarial o similar permitan excluir toda expectativa de privacidad» (art. 17.3 Ley 22/2018).

- Sistema Minerva: Este sistema, establecido por la citada Orden HFP/55/2023, detecta posibles casos de conflicto de intereses en los que puedan incurrir las personas que asuman funciones decisoras o particularmente relevantes en los procedimientos de contratación o de otorgamiento de subvenciones en el marco de la gestión de fondos del PRTR. El sistema emplea la información suscrita por los propios decisores controlados, mediante declaraciones de ausencia de conflictos de interés, cuyos datos son cruzados con los obrantes en las bases de datos de la Agencia Estatal de Administración Tributaria y los obtenidos, en su caso, a través de los convenios suscritos con los Colegios de Notarios y Registradores, a fin de detectar «las posibles relaciones familiares o vinculaciones societarias, directas o indirectas, en las que pueda haber un interés personal o económico susceptible de provocar un conflicto de interés» (art. 3.3 Orden HFP/55/2023). En caso de detectarse un conflicto de intereses, el sistema genera una bandera roja, para que el decisor afectado proceda a abstenerse de intervenir en el procedimiento correspondiente, aunque cabe la opción de formular alegaciones frente a la bandera, a fin de que el superior jerárquico decida si es procedente, o no, la abstención.

- Sistema Chronos-Eco (Sistema de captación dinámica de infracciones): Se trata del sistema empleado en el Área Metropolitana de Barcelona, para la detección, y propuesta de sanción, de infracciones relacionadas con el acceso no permitido a la zona de bajas emisiones, mediante la lectura automatizada de matrículas<sup>25</sup>. Este sistema, plenamente automatizado, propone la sanción sin que ninguna persona intervenga ni, por tanto, compruebe las imágenes que fundan la propuesta de sanción que se indica en la denuncia expedida de forma automatizada.

- Sistemas de control en materia de competencia en la contratación pública: En materia de competencia, se han conocido dos iniciativas similares para luchar contra prácticas anticompetitivas en la contratación pública y que, además, han sido premiadas: los sistemas Brava<sup>26</sup> y Ericca<sup>27</sup>. El sistema Brava (Bid Rigging Algorithm for Vigilance in Antitrust) es un sistema desarrollado y empleado por la Comisión Nacional de los Mercados y la Competencia para detectar, en las ofertas realizadas en el marco de procedimientos de contratación, aquellas que pueden ser potencialmente colusorias. Por su parte, el sistema ERICCA, o *Eina de Recerca Intel·ligent de la Col·lusió en la Contractació Administrativa* [Herramienta de Investigación Inteligente de la Colusión en la Contratación Administrativa], es un sistema desarrollado y empleado por la Autoridad Catalana de la Competencia que también se utiliza para detectar indicios de cárteles en contratos públicos en Cataluña que se empezó a desarrollar en 2021<sup>28</sup>.

- Sistema de control de la contratación de Localret: Se trata de un sistema informático ofrecido por el consorcio Localret a las administraciones locales catalanas para que puedan mejorar la gestión interna de la ejecución de los contratos públicos<sup>29</sup>, incluyendo, además, una función de control que genera alertas o avisos de forma automática, entre las que se incluyen alertas predefinidas de riesgos sobre posibles irregularidades, como fraccionamientos y repetición de contratos con las mismas empresas<sup>30</sup>.

<sup>25</sup>Véase [AMB \(2021\)](#).

<sup>26</sup>Véase [CNMC](#), «Premio a BRAVA, el proyecto de IA de la CNMC contra el fraude en contratación pública».

<sup>27</sup>Véase [Generalitat de Catalunya](#), «L'eina d'intel·ligència artificial de l'ACCO ha estat guardonada als Premis Alfons Ortuño d'innovació i bones pràctiques en la gestió pública».

<sup>28</sup>Tal y como se informa por la propia ACCO: [Autoritat Catalana de la Competència](#), «La Stanford University de Califòrnia convida l'Autoritat Catalana de la Competència a presentar l'ERICCA».

<sup>29</sup>Véase [Localret](#), «Webinar: Noves eines de seguiment informàtic i alertes en un entorn de dades per al control de la contractació pública local».

<sup>30</sup>Véase [Localret](#), «L'eina de seguiment, control i planificació de la contractació».

## 4 Propuesta de reforma normativa

A continuación, se presentan propuestas de reforma normativa, con los añadidos en letra cursiva, que derivan del análisis previo realizado en este capítulo.

En primer lugar, se propone añadir un apartado nuevo al art. 55 de la Ley 39/2015, que cubra específicamente la cuestión del cribado de resultados en los controles semiautomatizados, así como la posibilidad generalizada de poder iniciar procedimientos de comprobación a partir de los indicadores ofrecidos por un sistema algorítmico:

Artículo 55. Información y actuaciones previas

[...]

3. *Cuando, mediante sistemas semiautomatizados de control, basados en análisis de riesgos, detección de patrones o cualquier otra forma de señalación de alertas, se aconseje o sugiera la comprobación, inspección o seguimiento de hechos u actividades, podrán llevarse a cabo actuaciones de investigación, previa comprobación, por el órgano competente, de la verosimilitud del resultado generado por el sistema. En caso contrario, podrá ignorarse la alerta, como un falso positivo, con indicación del motivo por el que se trata de un falso positivo.*

En segundo lugar, se propone garantizar que tanto la formulación de recurso como la presentación de alegaciones (previas, pues, a la resolución administrativa) ante un acto derivado de una actuación de control plenamente automatizada se derivan a una persona para que las analice y, si procede, corrija el resultado injusto de la actuación automatizada. Para ello, se propone reformar el artículo 41 de la Ley 40/2015:

Artículo 41. Actuación administrativa automatizada

[...]

3. *En cualquier caso, la presentación de alegaciones y la interposición de recurso deberán ser informadas por el órgano que sea considerado responsable a estos efectos.*
4. *Cuando sea objeto de recurso un acto realizado íntegramente por medios electrónicos, el procedimiento de recurso y su resolución deberán realizarse sin intervención de actuación administrativa automatizada.*

En tercer lugar, se propone extender con carácter general la obligación de información sobre el uso de herramientas para el control automatizado en todos los procedimientos sancionadores, a partir del antecedente marcado por el Real Decreto 928/1998. Para ello, se propone modificar el art. 64 de la Ley 39/2015, añadiendo un nuevo apartado y modificando el actual último apartado del artículo, del siguiente modo:

Artículo 64. Acuerdo de iniciación en los procedimientos de naturaleza sancionadora

[...]

3. *Asimismo, cuando se haya comprobado y calificado los hechos constitutivos de infracción de forma automatizada, el acuerdo de iniciación deberá indicar también los medios utilizados para la comprobación de los hechos y la indicación expresa de que se trata de una actuación administrativa automatizada.*
4. *Excepcionalmente, cuando en el momento de dictar el acuerdo de iniciación no existan elementos suficientes para la calificación inicial de los hechos que motivan la incoación del procedimiento, la citada calificación podrá realizarse en una fase posterior mediante la elaboración de un Pliego de cargos, que deberá ser notificado a los interesados. Si la obtención de esos elementos suficientes para la calificación se realiza de forma automatizada, el Pliego de cargos deberá expresar los medios utilizados para la comprobación de los hechos y la indicación expresa de que se trata de*

*una actuación administrativa automatizada.*

En cuarto lugar, a fin de garantizar el equilibrio entre efectividad del control y transparencia suficiente, se propone incluir en la legislación de transparencia (Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, y leyes autonómicas de transparencia) la siguiente indicación en relación con la información pública objeto de publicidad activa<sup>31</sup>:

Artículo 6. Información institucional, organizativa y de planificación

[...]

3. *Los sujetos comprendidos en el ámbito de aplicación de este título publicarán información relativa a los sistemas algorítmicos empleados, con expresa indicación del órgano considerado responsable. Esta información debe incluir la descripción, en un lenguaje claro y sencillo, del diseño, funcionamiento y lógica del sistema, así como su finalidad y su incidencia en las decisiones públicas en el ámbito en que se emplea..*

En esta misma línea, por último, se propone garantizar el derecho de acceso a los resultados del sistema, para que la ciudadanía pueda conocer la efectividad de los sistemas de control:

Artículo 14. Límites al derecho de acceso

[...]

2. *La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso. En particular, en aquellos supuestos en que se*

*considere aplicable alguno de los límites previstos en el apartado 1.e) y .g) de este artículo, si la información solicitada se refiere al funcionamiento de un sistema algorítmico, deberá informarse sucintamente al menos sobre los ilícitos que el sistema pretende prevenir, detectar o sancionar, y si se solicita, asimismo la administración deberá proporcionar los datos agregados sobre el funcionamiento y efectividad del sistema en la prevención, detección, investigación o sanción de los ilícitos correspondientes.*

## 5 Justificación de la propuesta

En primer lugar se ha propuesto la reforma del art. 55 de la Ley 39/2015, con el objeto de dotar de mayor cobertura legal al uso, generalmente informal, de los sistemas semiautomatizados de control. De este modo, se considera oportuno incluir una previsión que cubra específicamente la cuestión del cribado, mediante supervisión humana, de resultados en los controles semiautomatizados, y que abra con carácter general la opción de poder iniciar procedimientos de comprobación a partir de los indicadores ofrecidos por un sistema algorítmico, sin que sea necesario que esta cuestión se aborde en todos los ámbitos sectoriales. Será, sin embargo, únicamente en esa legislación sectorial donde deban incorporarse salvaguardas específicas para minimizar el impacto de los falsos negativos, mediante otros sistemas para obtener información sobre posibles ilícitos, como, por ejemplo, denuncias o actuaciones de comprobación aleatorias.

En segundo lugar, se ha propuesto excluir la automatización en la tramitación de alegaciones o recursos frente a actuaciones derivadas de la actuación automatizada, para garantizar que una persona se encargue de validar el resultado del sistema algorítmico o, por el contrario, advierta y corrija los errores del sistema. Esos errores en ocasiones pueden ser muy evidentes para un ser humano (pensemos en el caso de las imágenes que justificaban la multa a un vehículo cargado en una grúa), y pueden ser corregidos de forma sencilla y rápida en el marco de sus respectivos procedimientos. En segundo lugar, esta intervención humana debería permitir la advertencia temprana de

<sup>31</sup>Se adoptan algunos elementos del redactado del art. 16.1 de la Ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la Comunitat Valenciana, que positiviza la transparencia algorítmica, si bien en ese caso se sitúa la relación de algoritmos en el bloque de información de relevancia jurídica. Por el especial papel que se da en esta propuesta de redacción a la intervención humana responsable de corregir los errores de funcionamiento del sistema, se ha situado en el bloque de información organizativa.

errores en el sistema, para proceder a la corrección y mejora de este de oficio, en cumplimiento de las exigencias de la buena administración, como se desprende de la resolución de la Sindicatura de Greuges de Barcelona ya mencionada.

La tercera propuesta normativa afecta al art. 64 de la Ley 39/2015, y tiene por objeto extender con carácter general la obligación de información sobre el uso de herramientas para el control automatizado en todos los procedimientos sancionadores. Esta reforma se inspira, en buena medida, en lo que prevé el Real Decreto 928/1998 en el marco de los procedimientos de inspección laboral.

A fin de evitar sortear las obligaciones de información sobre el sistema algorítmico, se ha previsto también incluir la misma obligación informativa en el Pliego de cargos, en caso de que los hechos se determinen, de forma automatizada, en un momento posterior a la iniciación del procedimiento sancionador.

Por último, se aborda la problemática de la transparencia algorítmica en el caso de los sistemas de control mediante dos inclusiones en la normativa de transparencia, referidas a la publicidad activa y al derecho de acceso en relación con estos sistemas, incorporando la obligación de buscar un equilibrio entre transparencia y opacidad. En efecto, y como ya he indicado en cuanto al nivel de transparencia exigible para los sistemas algorítmicos de control, me parece excesivo entender que todos los sistemas destinados a prevenir o detectar posibles infracciones están exentos del deber de publicidad activa y suponen una excepción al derecho de acceso. Por ello, considero que es adecuado ponderar conjuntamente la necesidad de información pública con la importancia de garantizar la efectividad del control administrativo mediante sistemas algorítmicos. Con ese objeto, la administración debería delimitar en cada caso qué datos concretos merecen realmente constituir una excepción al principio de transparencia, y quedar reservados para su uso y conocimiento interno únicamente, y cuáles pueden hacerse públicos para que exista un correcto conocimiento ciudadano de los sistemas que, posiblemente, puedan estar analizando sus datos y adoptando, o sugiriendo, actuaciones que le pueden afectar.

## 6 Los sistemas de control y el RIA

Por último, hay que hacer referencia a la posible inclusión de este tipo de sistemas como sistemas de alto riesgo, a los efectos del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armo-

nizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial, en adelante RIA).

El Anexo III RIA, en el apartado 6, cubre específicamente los sistemas de IA que se pueden considerar de alto riesgo por su uso en garantía del cumplimiento del Derecho. Si bien, a priori, podría entenderse que todos los sistemas de control de cumplimiento normativo y detección de incumplimientos empleados por las administraciones entran dentro de esta categoría, lo cierto es que el artículo 3 RIA define a las autoridades garantes del cumplimiento en relación con el control de incumplimientos de naturaleza delictiva, penal: “«garantía del cumplimiento del Derecho»: las actividades realizadas por las autoridades garantes del cumplimiento del Derecho, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas”. Así, el RIA parece excluir las herramientas de detección y sanción ante infracciones administrativas que empleen las autoridades u órganos administrativos sin competencia para investigar y castigar ilícitos penales, a pesar de que el uso de estos sistemas igualmente puede derivar en la aplicación de sanciones (aunque no penales). Por otro lado, en el apartado 5 del Anexo III RIA, se marcan como de alto riesgo aquellos sistemas que se empleen por las administraciones para reconocer el derecho a beneficiarse de servicios y prestaciones, así como “para conceder, reducir o retirar dichos servicios y prestaciones o reclamar su devolución”.

En definitiva, como se puede ver, los sistemas tratados en este capítulo, no entran en la categoría de alto riesgo de acuerdo con el RIA, si bien, como se ha visto, estos sistemas pueden generar de forma autónoma resultados con presunción de validez y eficacia jurídica (artículos 38 y 39 Ley 39/2015), y efectos desfavorables, como podría ser la propuesta de sanción automatizada. Así, desde el punto de vista del impacto en la ciudadanía, este tipo de sistemas no se diferencian en exceso de los sistemas que detectan ilícitos penales en tanto que también pueden tener eficacia sancionadora y, de hecho, incluso estos mismos sistemas de control administrativo pueden llegar a detectar ilícitos penales, como puede suceder si el fraude tributario o laboral que detectan los sistemas de la Agencia Tributaria o la Inspección de Trabajo y Seguridad Social constituyen un delito. En ese caso, obviamente, la autoridad administrativa no podrá sancionar, sino que deberá trasladarse el asunto al Min-

isterio Fiscal o autoridad judicial competente<sup>32</sup>. Por otro, entra en la categoría de alto riesgo aquel sistema que se emplee para reconocer o denegar situaciones favorables, como ya he indicado, por lo que no parece del todo razonable no considerar como tal aquellos que puedan imponer efectos desfavorables. Así, podría recomendarse, a nivel interno, extender la con-

sideración de alto riesgo a los sistemas administrativos de control automatizado o semiautomatizado, a efectos de aplicarles las garantías del RIA, en términos de transparencia y supervisión, entre otras, especialmente cuando puedan detectar ilícitos penales o generar de forma automatizada propuestas de sanción administrativa.

---

<sup>32</sup>Véase el art. 17.3 de la Ley 23/2015, de 21 de julio, Ordenadora del Sistema de Inspección de Trabajo y Seguridad Social.

## Referencias

- AEAT. (2024, Mayo). *Estrategia de Inteligencia Artificial*. Retrieved from [https://sede.agenciatributaria.gob.es/static\\_files/AEAT\\_Intranet/Gabinete/Estrategia\\_IA.pdf](https://sede.agenciatributaria.gob.es/static_files/AEAT_Intranet/Gabinete/Estrategia_IA.pdf)
- AMB. (2021). *Guía técnica para la implementación de zonas de bajas emisiones*. Retrieved from <https://revista.dgt.es/images/GUIA-ZBE.pdf>
- Baader, G., & Krcmar, H. (2018). Reducing false positives in fraud detection: Combining the red flag approach with process mining. *International Journal of Accounting Information Systems*, 31, 1-16.
- Capdeferro Villagrasa, O. (2019). Las herramientas inteligentes anticorrupción: Entre la aventura tecnológica y el orden jurídico. *Revista General de Derecho Administrativo*(50), 1-28.
- Cotino Hueso, L. (2023). Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida. *Revista Española de la Transparencia*(16), 17-63.
- Generalitat Valenciana. (2022). *Informe de evaluación del Plan de la Inspección General de Servicios 2022-2023*.
- Giray, L. (2024). The problem with false positives: AI detection unfairly accuses scholars of AI plagiarism. *The Serials Librarian*, 85(5-6), 181-189.
- Kroll, J. A., Huey, J., Barocas, S., Felten, E., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*, 165, 633-705.
- Martín Delgado, I. (2023). Inteligencia artificial y sector público: Retos, límites y medios. In E. Gamero Casado (Ed.), (p. 132-194). Valencia: Tirant Lo Blanch.
- Martínez Otero, J. M. (2024). Hipervigilancia administrativa y supervisión automatizada: Promesas, amenazas y criterios para valorar su oportunidad. *Revista Española de Derecho Administrativo*(231), 1-34.
- Mir Puigpelat, O. (2023). La automatización y el uso de algoritmos e inteligencia artificial en derecho administrativo comparado. *Revista General de Derecho Administrativo*(63), 1-9.
- Miranzo Díaz, J. (2023). *Inteligencia artificial y derecho administrativo*. Madrid: Tecnos.
- Poltoratskaia, V., & Fazekas, M. (2024). Routledge handbook of public procurement corruption. In S. Williams & J. Tillipman (Eds.), (p. 42-59). Oxon: Routledge.
- Ponce Solé, J. (2019). Inteligencia artificial, derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico. *Revista General de Derecho Administrativo*(50), 1-52.
- Ponce Solé, J. (2024). Inteligencia artificial, decisiones administrativas discrecionales totalmente automatizadas y alcance del control judicial: ¿indiferencia, insuficiencia o deferencia. *Revista de Derecho Público: Teoría y Método*, 9, 9-56.
- Rachovitsa, A., & Johann, N. (2022). The human rights implications of the use of AI in the digital welfare state: Lessons learned from the Dutch SyRI case. *Human Rights Law Review*, 22(2), 1-15.
- Ranchordás, S., & Schuurmans, Y. (2020). Outsourcing the welfare state: The role of private actors in welfare fraud investigations. *European Journal of Comparative Law and Governance*, 7(1), 5-42.