# Retos legais do uso do *big data* na selección de suxeitos a investigar pola Inspección de Traballo e da Seguridade Social

# Retos legales del uso del *big data* en la selección de sujetos a investigar por la Inspección de Trabajo y de la Seguridad Social

# Legal challenges of the use of big data in the selection of subjects to be investigated by the Labour and Social Security Inspectorate

Regap 59

ADRIÁN TODOLÍ SIGNES

Profesor ayudante doctor de Derecho del Trabajo y de la Seguridad Social
Universidad de Valencia
Orcid 0000-0001-7538-4764
adrian.todoli@uv.es

Recibido: 19/05/2020 | Aceptado: 03/07/2020
DOI: https://doi.org/10.36402/regap.v0i59.4354



**Resumo:** Planear axeitadamente unha estratexia de inspeccións é clave para detectar a fraude *a posteriori*, así como para proactivamente previr que existan incumprimentos da norma. Entre as fórmulas tradicionais para seleccionar os suxeitos obxecto dunha inspección introduciuse recentemente o uso do *big data* e os algoritmos. Esta tecnoloxía promete mellorar os "acertos" á hora de seleccionar que empresas se van investigar por posibles ilícitos ou fraudes. Non obstante, isto pode presentar problemas xurídicos respecto á protección dos datos usados pola Administración e tamén na aplicación do principio de igualdade e non discriminación na selección de obxectivos da Inspección. Habitualmente, as normas para evitar vulneración de dereitos fundamentais dos cidadáns exixen transparencia da Administración, a chamada "transparencia algorítmica". Non obstante, como se discute neste traballo, a dita transparencia podería frustrar os obxectivos perseguidos no uso da ferramenta. Neste artigo analízase, por unha banda, o uso do *big data* na planificación estratéxica de campañas de inspección e, por outra, os retos legais que iso representa, con especial recoñecemento dos principios aplicables e a incipiente doutrina xudicial en países dos nosos arredores.

**Palabras clave:** Algoritmos e Administración pública, *big data*, selección de suxeitos a investigar, transparencia algorítmica, IA e Administración pública, Inspección de Traballo e Seguridade Social.

**Resumen:** Planear adecuadamente una estrategia de inspecciones es clave para detectar el fraude a posteriori, así como para proactivamente prevenir que existan incumplimientos de la norma. Entre las fórmulas tradicionales para seleccionar los sujetos objeto de una inspección se ha introducido recientemente el uso del *big data* y los algoritmos. Esta tecnología promete mejorar los "aciertos" a la hora de seleccionar qué empresas se van a investigar por posibles ilícitos o fraudes. No obstante, esto puede plantear problemas jurídicos respecto a la protección de los datos usados por la Administración y también en la aplicación del principio de igualdad y no discriminación en la selección de objetivos de la Inspección.

Habitualmente, las normas para evitar vulneración de derechos fundamentales de los ciudadanos exigen transparencia de la Administración, la llamada "transparencia algorítmica". Sin embargo, como se discute en este trabajo, dicha transparencia podría frustrar los objetivos perseguidos en el uso de la herramienta. En este artículo se analiza, de un lado, el uso del *big data* en la planificación estratégica de campañas de inspección y, de otro, los retos legales que ello representa, con especial reconocimiento de los principios aplicables y la incipiente doctrina judicial en países de nuestro entorno.
**Palabras clave:** Algoritmos y Administración pública, *big data*, selección de sujetos a investigar, transparencia algorítmica, IA y Administración pública, Inspección de Trabajo y Seguridad Social.

**Abstract:** Properly planning an inspection strategy is key to detecting fraud *a posteriori*, as well as proactively preventing non-compliance with the standard. Among the traditional formulas for selecting the subjects to be inspected, the use of *big data* and algorithms has recently been introduced. This technology promises to improve the "hits" when selecting which companies to investigate for possible crimes or fraud. However, this may raise legal problems regarding the protection of the data used by the Administration and also in the application of the principle of equality and non-discrimination in the selection of objectives of the Inspection. Usually, the rules to avoid violation of Fundamental Rights of citizens require transparency from the Administration, the so-called "algorithmic transparency". However, as discussed in this work, such transparency could frustrate the objectives pursued in the use of the tool. This work analyzes, on the one hand, the use of big data in the strategic planning of inspection campaigns and, on the other, the legal challenges that this represents, with special recognition of the applicable principles and the incipient judicial doctrine in countries around us.
**Key words:** Algorithms and Public Administration, big data, selection of subjects to investigate, algorithmic transparency, AI and Public Administration, Labour and Social Security Inspectorate.



# 1 La selección de sujetos objeto de una investigación

El derecho del trabajo y de la seguridad social parte, como presupuesto habilitante de su propia existencia, de un desequilibrio de poder entre las partes sujetas al mismo. Esto no solamente tiene efectos en materia de negociación de condiciones de trabajo, sino también en las posibilidades de la parte débil de exigir el cumplimiento de sus derechos. Por esta razón, la construcción de ordenamiento social, desde sus orígenes, ha venido acompañado de la necesidad de una vigilancia y control de carácter público de su cumplimiento. Esto se ha realizado y se realiza, principalmente, a través de la Inspección de Trabajo y de la Seguridad Social.

Actualmente existen diferentes fórmulas para conseguir el cumplimiento de la norma por parte de los obligados; sin embargo, la realización de indagaciones y la

propuesta de sanciones en caso de descubrir un incumplimiento siguen siendo las principales herramientas con las que cuenta el Estado para hacer cumplir sus normas[1].

Un exitoso programa de inspecciones no tiene como consecuencia solamente los efectos directos en cada acción individual (en términos de conseguir el cumplimiento del inspeccionado, por ejemplo, la recaudación obtenida de esa inspección). Por el contrario, existen otros efectos indirectos, en muchos sentidos más relevantes, para el mantenimiento general del nivel de cumplimiento de las normas[2].

En efecto, la existencia de un sistema eficiente de control que localice y castigue a los que infringen la norma convencerá al resto de obligados que cumplirla redunda en su beneficio[3]. A su vez, incrementará la percepción de poder ser inspeccionado, algo que, de acuerdo con el modelo estándar de cumplimiento de las normas, conducirá a un incremento del cumplimiento voluntario[4]. Por último, un sistema de inspección que audite y castigue a los que contravienen la norma pondrá fin a la competencia desleal entre las empresas, eliminando una posible necesidad de incumplir para poder competir en el mercado en igualdad de condiciones.

No obstante, a nadie se le escapa que el proceso de inspección es un proceso intrusivo no muy bienvenido por las empresas[5]. Incluso para las empresas que no infringen ninguna normativa, y no reciben ningún requerimiento ni sanción, la presencia de la Inspección en sus instalaciones y la solicitud de información es una intromisión que altera la normal convivencia dentro de esta. Sumado a lo anterior, las inspecciones son un procedimiento costoso, tanto en capital humano como financiero para el Estado[6].

La Inspección debe, por esta razón, usar sus limitados recursos de manera prudente para obtener el máximo nivel de cumplimiento con la mínima intrusión y los mínimos costes[7]. Planear adecuadamente una estrategia de inspecciones es clave para detectar el fraude a posteriori, así como para proactivamente prevenir que existan incumplimientos de la norma. Es decir, partiendo de la hipótesis de que inspeccionar a una empresa que cumple con la norma proporciona pocos beneficios a la prevención del fraude, la selección de los sujetos objeto de la inspección será esencial. El objetivo,



1 OCDE, *Compliance Risk Management: Audit Case Selection Systems*, OECD Press, París, 2004, p. 6.

2 OCDE, *Compliance Risk Management: Audit Case Selection* Systems, cit., p. 7.

3 GUPTA, M. y NAGADEVARA, V., "Audit Selection Strategy for Improving Tax Compliance – Application of Data Mining Techniques", *Foundations of E-Government – Conference Proceedings, 11th International Conference on e-Governance*, Hyderabad, India, 2007, p. 378.

4 BECKER, G., "Crime and Punishment: An Economic Approach", *Journal of Political Economy*, n. 76-2, 1968, pp. 169-217; SRINIVASAN, T.N., "Tax Evasion: A model", *Journal of Public Economics*, n. 2, issue 4, 1973, pp. 339-346; YITZHAKI, S., "Income tax evasion: A theoretical analysis", *Journal of Public Economics*, n. 3, issue 2, 1974. ALLINGHAM, M.G. y SANDMO, A., "Income Tax Evasion: A Theoretical Analysis", *Journal of Public Economics*, n. 1, 1972, pp. 323-338.

5 GUPTA, M. y NAGADEVARA, V., "Audit Selection Strategy for Improving Tax Compliance – Application of Data Mining Techniques", cit., p. 378.

6 BONCHI, F., GIANNOTTI, F., MAINETTO, G. y PEDRESCHI, D., "A classification-based methodology for planning audit strategies in fraud detection", *KDD '99: Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining*, 1999, p. 176. Disponible en: https://dl.acm.org/doi/10.1145/312129.312224 (Consultado el 6 de abril de 2020).

7 GUPTA, M. y NAGADEVARA, V., "Audit Selection Strategy for Improving Tax Compliance – Application of Data Mining Techniques", cit., p. 378.

pues, será planificar estratégicamente la actuación inspectora de tal forma que cada inspección se realice sobre una empresa que incumpla.

En este sentido, parece que hay campo para la mejora en algunos sectores. De acuerdo con el Informe anual 2018 de la Inspección de Trabajo y Seguridad Social, en materia de contratación de trabajadores, la actividad planificada ha arrojado los siguientes resultados. De un total de 55.640 actuaciones, se ha detectado la comisión de 3.877 infracciones sancionables. Ello significa que el "acierto", a la hora de seleccionar a las empresas objeto de la inspección durante una campaña dirigida, ha sido del 6%[8] aproximadamente. Respecto al tiempo de trabajo, se realizaron 20.465 actuaciones con un resultado de 5.230 infracciones[9], lo que implica un éxito del 25%.

En general, en materia de empleo y relaciones laborales, incluyendo no solo la actividad planificada, sino también aquella realizada como respuesta a una denuncia, el nivel de acierto a la hora de realizar una inspección que terminara en la detección de un incumplimiento sancionable ha sido del 12%[10]. Ello implica, en sentido contrario, que se han usado recursos de la Inspección y se ha alterado el normal funcionamiento de una empresa en un 88% de los casos, sin que dicho comportamiento viniera justificado por la gravedad del incumplimiento de la misma[11].

Por otro lado, existe otro fenómeno que merece específica atención. En materia de prevención de riesgos laborales en el sector de la construcción, del total de 28.134 órdenes de servicio, la suma de requerimientos e infracciones –aquí la memoria de la Inspección no da datos desglosados– ha sido de 32.345. Ello significa un acierto del 114% en la actuación. Este no es un fenómeno específico de la construcción, dado que el acierto en el resto de sectores se sitúa en el 126%. Esto es, ***grosso modo*** y en términos generales, en cada empresa visitada se han detectado de media 1,26 incumplimientos. Estos datos arrojan conclusiones preocupantes.

De un lado, podría implicar un gran acierto por parte de la Inspección de Trabajo a la hora de seleccionar qué empresas son auditadas en materia de prevención de riesgos. Sin embargo, sin información alguna que haga pensar que existe una manera distinta de seleccionar las empresas inspeccionadas en esta materia de las anteriores que se acaban de ver, probablemente más bien suponga un incumplimiento sistemático en esta materia. No obstante, ello no significa que la planificación estratégica resulte innecesaria en esta materia, sino que el objetivo de la planificación en materia de

---

8 Ello suponiendo que cada infracción ha sido a una única empresa, siendo posible también que las sanciones por contratación fraudulenta de trabajadores temporales se hayan concentrado en unas pocas empresas, lo que reduciría todavía más el nivel de acierto. Por otro lado, la memoria también recoge un total de 21.199 requerimientos. Ello significa, probablemente, que se han encontrado irregularidades en esas empresas, aunque de insuficiente relevancia como para ser sancionadas. Contando también con los requerimientos, el nivel de "acierto" se situaría en el 45%.

9 Igualmente, en este caso, se podrían añadir los 6.040 requerimientos que se realizaron en esta materia, arrojando un resultado de acierto en este caso del 55%.

10 Teniendo en cuenta los requerimientos el nivel de éxito sería del 40%.

11 Todo ello a los ojos de la propia Inspección de Trabajo y de la Seguridad Social, que, tras iniciar la inspección, decidió no sancionar. Por supuesto, también es posible que la decisión final de no sancionar viniera causada no porque no exista incumplimiento que merezca ser sancionado, sino por la falta de pruebas que lo acrediten. No obstante, este argumento no resta razones a lo aquí sustentado. Si la Inspección audita una empresa y finalmente no encuentra pruebas suficientes para sancionar, no se habrá producido el efecto indirecto en términos de prevención general tan necesario en estas actuaciones y en el uso de recursos.

prevención debería ser distinto. En este sentido, no se debería pretender encontrar "algún" incumplimiento, del tipo que sea, por cada inspección, sino seleccionar las empresas que realizan los incumplimientos más graves.

En efecto, la planificación estratégica debe pretender siempre maximizar los resultados de la actuación inspectora[12]. Por esto, en la planificación, el objetivo será decidir auditar aquellas empresas donde existe un riesgo mayor de un incumplimiento ***grave***. En materia de prevención de riesgos laborales, esta diferenciación es sencilla de observar. No será lo mismo, a la hora de decidir auditar una empresa u otra, que una incumpla una normativa que implique un alto riesgo de accidente mortal que otra que implique riesgos menores. No se pone en duda la necesidad de auditar todas las empresas incumplidoras. No obstante, siendo los recursos escasos, puede tener sentido priorizar estratégicamente la reducción de los accidentes más graves.

Por esta razón, en los últimos años se ha impulsado, desde muchas administraciones[13], el uso de tecnologías de la información –***big data***, ***data mining***, ***machine learning***, algoritmos, inteligencia artificial, etc.– con objeto de mejorar la selección de las empresas a inspeccionar o de objetivos de las campañas, basándose en el procesamiento automatizado de los datos.

Este trabajo tiene como objetivo discutir los beneficios y limitaciones del uso de la tecnología del ***big data*** como forma de tomar decisiones respecto a qué empresas inspeccionar en materia de trabajo y seguridad social. Para ello, en el epígrafe 2 se analizarán los distintos modelos de selección de empresas objeto de esta inspección. El tercer epígrafe se dedicará a las mecánicas de funcionamiento del sistema de valoración del fraude. El cuarto, a la necesidad de evaluar los resultados. El quinto contempla los retos legales en materia de protección de datos, intimidad y regulación antidiscriminatoria de la implantación del sistema. El trabajo termina concluyendo con las ventajas y límites de esta tecnología en materia de prevención del fraude.



## 2 Retos legales: protección de datos y derechos fundamentales afectados

El uso de algoritmos, la clasificación de los sujetos mediante perfiles de riesgo de incumplimiento y el tratamiento de datos de forma automatizada a través de las técnicas descritas en este trabajo con objeto de seleccionar las empresas a inspeccionar puede plantear múltiples problemas jurídicos. De un lado, las normas de protección de datos y, de otro, las normas antidiscriminación y de protección de la intimidad pueden suponer límites jurídicos al uso de estas técnicas.

El análisis particularizado de la legalidad del empleo de estas técnicas difícilmente puede hacerse en este momento de forma abstracta y ***a priori*** sin conocer exactamente

[12] BONCHI, F., GIANNOTTI, F., MAINETTO, G. y PEDRESCHI, D., "A classification-based methodology for planning audit strategies in fraud detection", cit.

[13] COMISIÓN EUROPEA, ***Risk Management Guide for Tax Administrations,*** Bruselas, 2006. Disponible en:https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/taxation/tax_cooperation/gen_overview/risk_management_guide_for_tax_administrations_en.pdf. OCDE, ***OECD Regulatory Enforcement and Inspections Toolkit***, París, 2018, p. 13.

las mecánicas y el tipo de información que el sistema utiliza. Por ello, el presente epígrafe se limita a señalar los retos jurídicos que puede plantear este uso y los principios legales que deben orientar la adopción de estas técnicas por parte de la Inspección. Para efectuar este análisis, primero se debe dividir la cuestión entre los sujetos afectados: de un lado, el uso del ***big data*** para seleccionar personas jurídicas o empresas y, de otro, para seleccionar profesionales autónomos o personas individuales.

## 2.1 Aplicación del *big data* para seleccionar personas jurídicas o empresas

La necesaria segmentación respecto a la selección de personas jurídicas frente a la selección de personas físicas parte de la propia división realizada por la normativa. En efecto, el RGPD se circunscribe a la protección de ***datos personales***, incluyendo solamente los datos de las personas físicas y excluyendo de su ámbito de aplicación los datos de las personas jurídicas (art. 1 y 2 RGPD)[14].

De esta forma, el tratamiento automatizado de datos de las empresas y su procesamiento a través de técnicas de ***big data*** no viene protegido por esta normativa[15]. Serán los principios generales, la obligación de la Administración de regirse bajo el principio de legalidad, de igualdad de trato y la prohibición de arbitrariedad los que determinarán las posibilidades de uso de las mismas. Ello lleva a que, en la utilización del ***big data*** para la selección de empresas a investigar, a falta de normativa específica en materia de protección de datos, se apliquen los controles clásicos y habituales en la Administración.

## 2.2 Aplicación para la selección de personas físicas o autónomos

En materia de vigilancia del cumplimiento de la normativa social, la Inspección también es la encargada de controlar el posible fraude de prestaciones sociales recibidas por personas físicas y el cumplimiento de la normativa laboral por parte de profesionales autónomos respecto a la Seguridad Social propia y en cuanto a su posición como empleador.

### 2.2.1 Protección de datos y autónomos

Una primera cuestión que surge es si la normativa en materia de protección de datos personales se aplica a los autónomos y profesionales en el ejercicio de su profesión. A este respecto surgen dudas dado que, a pesar de que son personas físicas, interactúan como empresarios en el mercado. Esta cuestión ha sido tratada por la doctrina

[14] Expresamente, el artículo 4 define «datos personales» como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse".

[15] No obstante, téngase en cuenta que los datos de la empresa o de la actividad empresarial quedarán excluidos de la aplicación de esta normativa, pero no los datos de los profesionales y trabajadores (persona física) que se encuentren integrados en la organización; ver Informe jurídico AEPD 2008/0371.

judicial y llegó a la conclusión de que se entiende que solamente están excluidos del ámbito de aplicación de la normativa de protección de datos aquellos profesionales que ejercen su actividad bajo la forma de persona jurídica[16].

En efecto, la Sentencia de la Audiencia Nacional de 21 de noviembre de 2002 (rec. 881/2000) considera que la publicación de los datos identificativos de los arquitectos está protegida por la LOPD, puesto que son datos que "*se refieren a profesionales que no ejercen su actividad bajo forma de empresa, no ostentando en consecuencia la condición de comerciante a la que se refieren los artículos primero y siguientes del Código de comercio*".

En el mismo sentido, la SAN de 11 de febrero de 2004 (rec. 119/2002) señala que "*en el caso examinado el dato del afectado, aunque se refiera al lugar de ejercicio de su profesión es un dato de una persona física con una actividad profesional, cuya protección cae en la órbita de la Ley orgánica 15/1999*".

También el Tribunal Supremo –Sala 3.ª– en Sentencia de 20 de febrero de 2007 (rec. 732/2003) es del mismo parecer al establecer que "*Es claro que los arquitectos y promotores a que se refiere el litigio participan de la naturaleza de personas físicas y que no dejan de serlo por su condición de profesionales o agentes que intervienen en el mercado de la construcción, por lo que los datos personales relativos a los mismos quedan amparados y sujetos en cuanto a su tratamiento informatizado a las previsiones de la LORTAD; y es que desde este punto de vista subjetivo la exclusión del ámbito de aplicación de la LORTAD no viene determinado por el carácter profesional o no del afectado o titular de los datos objeto de tratamiento, sino por la naturaleza de persona física o jurídica titular de los datos, en cuanto sólo las personas físicas se consideran titulares de los derechos a que se refiere el art. 18.4 de la Constitución*".

De esta forma, los datos profesionales de los trabajadores autónomos –en cuanto son personas físicas– estarán amparados por la normativa en materia de protección de datos personales vigente.



# 3 Límites jurídicos a la aplicación del *big data* en la lucha contra el fraude laboral

## 3.1 Decisiones automatizadas y protección de datos

Aclarado que la normativa en materia de protección de datos será aplicable tanto a profesionales autónomos como a personas físicas –perceptores de prestaciones sociales–, se va ahora a analizar el régimen jurídico aplicable.

El RGPD, en su artículo 6.1 e), establece que el tratamiento de datos de las personas físicas es lícito si "*es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*". Así pues, con el amparo de la Ley 23/2015, de 21 de julio, ordenadora del Sistema de

[16] AEPD R/00598/2007.

Inspección de Trabajo y Seguridad Social –concretamente su artículo 18.2 y 18.4–, la recogida y tratamiento de estos datos será lícita.

Adicionalmente, aunque la recogida de datos y su tratamiento sean lícitos conforme se acaba de ver, el artículo 22 del RGPD fija una regla específica para la toma de decisiones basadas únicamente en este tratamiento automatizado o en la elaboración de perfiles. En concreto, este artículo prohíbe[17] que una decisión final, que tenga efectos jurídicos sobre el sujeto[18], esté basada únicamente en ese tratamiento automatizado o perfil elaborado por el algoritmo sin intervención humana. Esto puede afectar de lleno a las posibilidades de seleccionar automatizadamente (o mediante perfiles de personas físicas o autónomos) los sujetos a inspeccionar.

No obstante, esta prohibición se aplica solamente si no existe ningún tipo de intervención humana en la selección final del sujeto objeto de la inspección. En efecto, el artículo 22 RGPD que aquí se analiza solamente prohíbe la "decisión basada únicamente en el tratamiento automatizado". Por esta razón, si existe intervención humana ***significativa*** en la toma de decisión, no será de aplicación esta imposibilidad[19].

En este sentido, en los casos en los que la decisión final queda en manos del inspector, cuya decisión será tomada conforme a su experiencia usando únicamente el índice de riesgo de incumplimiento como un factor a tener en cuenta, no parece que nos encontremos en el supuesto prohibido del artículo 22 RGPD. De la misma forma, si los planes estratégicos y las campañas son decididos por los responsables de la Inspección, tampoco parece que se estuviera ante el presente supuesto[20].

En cualquier caso, una vez más, el artículo 22 RGPD establece excepciones a su aplicación. El reglamento permite que se elaboren decisiones totalmente automatizadas, siempre que ello venga autorizado por el derecho nacional (art. 22.1 b RGPD). Así, el artículo 16.3 de la Ley 23/2015 contempla la posibilidad de que la Inspección reciba datos cedidos por la Agencia Tributaria y la Seguridad Social, incluyendo los datos personales objeto de tratamiento automatizado. Esta parece una habilitación suficiente teniendo en cuenta que la cesión de datos siempre es un ejercicio más intenso

---

17 Literalmente, el artículo 22 RGPD no establece una prohibición, sino que la regla se configura como "el derecho a no ser objeto de este tipo de decisiones". No obstante, como ya se ha discutido y argumentado en otro lugar (TODOLÍ SIGNES, A., "La gobernanza colectiva de la protección de datos en las relaciones laborales: ***big data***, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos", ***Revista de Derecho Social***, n. 84, 2018), este derecho debe entenderse como una prohibición tal y como lo interpreta el GT29, ***Guidelines on Automated individual decisión-making and Profiling for the purposes of Regulation 2016***/679, 2016 (adoptadas el 3 de octubre de 2017), p. 13. Esto es, se configura como una prohibición –sin necesidad de reclamar activamente el derecho– a los responsables de datos de tomar las decisiones con esta metodología automatizada.

18 En mi opinión, no parece que haya dudas de que abrir una inspección sobre una persona física o autónomo tiene efectos jurídicos (ej., obligación de responder solicitudes de información, etc.), por lo que este criterio estaría cumplido.

19 TODOLÍ SIGNES, A., "La gobernanza colectiva de la protección de datos en las relaciones laborales: ***big data***, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos", cit.

20 En cualquier caso, recuérdese que la intervención humana en la toma de decisión debe ser significativa. Se está ante un concepto jurídico indeterminado en el que se deberá analizar caso a caso el nivel de intervención. Lo que está claro es que, si los responsables de la Inspección se limitan a validar la decisión tomada por el ***big data*** en todas las ocasiones, podría no haber intervención suficiente para excluir estas protecciones. En este sentido, para saber si el nivel de intervención humana es "significativo", habrá que valorar con qué frecuencia el responsable de recursos humanos adopta decisiones finales en un sentido distinto al planteado por el algoritmo o la IA; TODOLÍ SIGNES, A., "La gobernanza colectiva de la protección de datos en las relaciones laborales: ***big data***, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos", cit.

que el mero tratamiento; así pues, se podría sostener que quien puede lo más puede lo menos (si se permite legalmente la cesión de los datos, se permite su tratamiento automatizado). No obstante, en caso de que se desee poder seleccionar a los sujetos objeto de la inspección sin intervención humana alguna, sería recomendable una actualización de la normativa nacional que expresamente aclarare la posibilidad del tratamiento automatizado y la elaboración de perfiles con este objetivo y estableciera garantías suficientes de transparencia y antidiscriminación.

## 3.2 Garantías frente a la toma de decisiones automatizada

La Comisión Europea, en su ***Libro blanco sobre inteligencia artificial***[21] alerta de una serie de peligros existente en el uso de la IA, entre los que se encuentra la opacidad de algunos de estos sistemas de ***big data***, decisiones algorítmicas discriminatorias contra colectivos protegidos o decisiones erróneas por un mal diseño de los algoritmos[22]. Con objeto de evitar estos perjuicios, la Comisión Europea (2020) sostiene la necesidad de establecer garantías a favor de los afectados por un sistema de inteligencia artificial.

La regulación propuesta parte de que no todos los sistemas tienen la misma incidencia sobre esos derechos fundamentales; por ello, se plantea un sistema de garantías distinto dependiendo del riesgo que tenga la IA de afectar a esos derechos fundamentales. De esta forma, podría haber hasta cinco niveles basados en el riesgo de que una inteligencia artificial afecte o vulnere derechos fundamentales. Esto es, dependiendo de sus potenciales efectos, requeriría desde la ausencia de garantías en el caso de los sistemas de IA más inocuos hasta la prohibición absoluta en el caso de los sistemas de inteligencia artificial más peligrosos.

En efecto, la doctrina viene señalando desde hace tiempo la posibilidad de que los sistemas de decisión automatizada conculquen derechos fundamentales y la necesidad de garantías en su uso[23]. En este sentido, puede indicarse como ejemplo el uso por parte de EE. UU. de un algoritmo para determinar la probabilidad de reincidencia de un sujeto que ha cometido un delito. En este caso, los jueces utilizan esa probabilidad para determinar la duración de las penas privativas de libertad. Dado que la metodología y el algoritmo usados para la evaluación del riesgo de reincidencia son desconocidos para el defendido, se alegó violación del derecho de defensa y al proceso debido dada la imposibilidad de impugnar esa valoración del riesgo ni de saber si esa valoración estaba sesgada o era directamente discriminatoria (especialmente contra personas de color en EE. UU.).



---

21 COMISIÓN EUROPEA, *Libro blanco sobre la inteligencia artificial - Un enfoque europeo para la excelencia y la confianza,* COM (2020) 65 final, Bruselas, 2020.

22 En el mismo sentido se pronuncian CERRILLO I MARTÍNEZ, A., "El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?", *Revista General de Derecho Administrativo,* n. 50, 2019; COTINO HUESO, L., "Derecho y garantías ante el uso público y privado de inteligencia artificial, robótica y *big data*", Bauzá Reilly, M. (dir.), *El Derecho de las Tics en Latinoamérica,* La Ley, Uruguay, 2019; PONCE SOLÉ, J., "Inteligencia artificial, derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", *Revista General de Derecho Administrativo,* n. 50, 2019.

23 CRAWFORD, K. y SCHULTZ, J., "Big data and due process: Towards a framework to redress predictive privacy harms", *Boston College Law Review,* n. 55 (1), 2014.

No obstante, el Tribunal Supremo del estado de Wisconsin en la Sentencia State *v.* Loomis[24] consideró que el hecho de que el acusado no supiera la metodología de la evaluación del riesgo usada por el algoritmo no viola su derecho a un proceso debido ni a una sentencia individualizada, dado que el informe solamente es uno más de los factores tenidos en cuenta por el juez para fijar la sentencia definitiva. Además, en este caso, se sostiene que no es posible entregar la información sobre el funcionamiento del algoritmo ni la metodología usada, puesto que es un "secreto de empresa" (los informes son contratados por la Administración de justicia a una empresa privada).

Ante estas conclusiones, la doctrina ha criticado la sentencia y ha sostenido la necesidad de que exista total transparencia en la metodología usada por el algoritmo con objeto de poder impugnar el informe y conocer si esta estaba utilizando criterios discriminatorios para realizar la valoración final del riesgo de reincidencia (ej., color de piel)[25]. En efecto, se debe estar de acuerdo con estas críticas, y es que, cuando la libertad de circulación de una persona está en juego, la libertad de empresa o el secreto empresarial no puede ser argumentación suficiente para permitir una opacidad que impida conocer posibles discriminaciones.

Por esta razón, el RGPD señala que, incluso cuando una ley nacional autorice el uso de mecanismos informáticos para tomar decisiones automatizadas, será necesario que esta misma normativa fije controles y salvaguardas de los derechos y libertades de los sujetos afectados. No obstante, conforme al criterio mantenido por la Comisión Europea[26] en su calificación de los tipos de algoritmos según sus consecuencias, parece claro que esas garantías deberán ser proporcionales a los efectos, más o menos intensos, que las decisiones automatizadas tengan sobre el sujeto.

### 3.3 Discrecionalidad administrativa en la elección de sujetos a investigar y garantías frente a la arbitrariedad o discriminación

La elección del sujeto a investigar, así como la orientación mediante planes de inspección de la misma, se califican jurídicamente de actos discrecionales[27]. De esta forma, el inspector podrá elegir, basándose en su experiencia –como se hace tradicionalmente–, o en otros datos o informaciones, los sujetos objeto de su trabajo. De la misma forma, la confección de planes estratégicos y operativos desde los mandos jerárquicos de la inspección solamente viene a elevar esa potestad discrecional a instancias superiores. En este sentido, se admite pacíficamente la inclusión en los

[24] State *v.* Loomis, 881 N.W.2d 749 (Wis. 2016), accesible *online* en: https://law.justia. com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html (Consultado el 17 de julio de 2018).

[25] BOIX PALOP, A., "Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones", *Revista de Derecho Público: Teoría y Método*, n. 1, 2020. FREEMAN, K., "Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State *v.* Loomis", *North Carolina Journal of Law & Technology*, n. 18, 2016; MARTÍNEZ GARAY, L., "Peligrosidad, algoritmos y *due process*: el caso State *vs.* Loomis", *Revista de Derecho Penal y Criminología*, n. 20, 2018, pp. 485-502.

[26] COMISIÓN EUROPEA, *Libro blanco sobre la inteligencia artificial - Un enfoque europeo para la excelencia y la confianza*, cit.

[27] BERMEJO VERA, J., "La Administración inspectora", *Revista de Administración Pública*, n. 147, 1998, p. 54; REBOLLO PUIG, M., "La actividad inspectora", Díez Sánchez, J.J. (coord.), *Actas del VIII Congreso de la Asociación Española de Profesores de Derecho Administrativo: La función inspectora*, INAP, Madrid, 2013, p. 51.

mismos de criterios de oportunidad y el establecimiento de prioridades y estrategias para aplicar con la máxima eficiencia recursos limitados de esta[28].

Hasta aquí no parece que exista límite legal alguno para el uso del ***big data*** como soporte para la toma de dichas decisiones. No obstante, no está de más recordar que la discrecionalidad no puede significar arbitrariedad y que tiene límites, con objeto de evitar abusos y discriminaciones[29]. Así, de la misma forma que en la elección de los sujetos a inspeccionar no sería lícito realizarla basándose exclusivamente en la nacionalidad de la empresa o de la persona física, tampoco el ***big data*** podría llevarnos a dicha conclusión –ni siquiera de forma indirecta– sin que existan razones objetivas distintas al criterio discriminatorio que lo justifique.

Así pues, se debe partir de que, ***a priori***, no existe diferente régimen jurídico aplicable cuando la decisión es tomada fundamentándose en la experiencia del inspector, en los datos existentes, en criterios de oportunidad o en el ***big data***. Esto es, lo importante no reside en la forma o procedimiento elegido para tomar la decisión, sino en comprobar que el resultado de esta –la decisión– no sea arbitrario o discriminatorio.

El problema radica en las posibilidades de defensa del sujeto investigado. En efecto, en un caso u otro, el sujeto seleccionado desconocerá las razones por las que ha salido elegido, lo que hará materialmente imposible demostrar en juicio un trato sesgado o discriminatorio de la Inspección. Por esta razón, el artículo 20.2 de la Ley 23/2015 establece que es necesario garantizar la efectividad de los principios de igualdad de trato y no discriminación en el ejercicio de la actividad inspectora. O sea, es la Administración la obligada a asegurarse de que las decisiones no se toman en contra del principio de igualdad. A su vez, este artículo garantiza la publicación de las instrucciones de organización de servicios, de los criterios operativos generales y de los criterios técnicos vinculantes.

De esta forma, de un lado, la Administración tiene la obligación de asegurar que el ***big data*** no esté dando como resultado una elección discriminatoria o sin fundamento suficiente; por otro lado, será necesario garantizar cierto grado de transparencia en los criterios utilizados por el ***big data*** para tomar sus decisiones y establecer los porcentajes de riesgo de incumplimiento de cada empresa o de los distintos sectores.

Esto es, no parece que sea suficiente indicar que se ha elegido una empresa –o un sector si hablamos de un plan estratégico– porque la herramienta informática indica que tiene mayor riesgo de incumplir. Por el contrario, la Administración tendrá la obligación de asegurar que el resultado final del índice de riesgo de incumplimientos no está basado en criterios prohibidos (nacionalidad de la empresa o persona física, sindicación o no, etc.). La analogía con las herramientas de selección tradicionales hasta el momento es sencilla, y es que, conforme al principio de igualdad, la Administración también debe asegurarse de que un inspector no actúe motivado por razones arbitrarias y discriminatorias.

De esta forma, igual que, de acuerdo con la normativa actual, los criterios operativos generales deben ser publicados para garantizar la no arbitrariedad, parece

[28] RIVERO ORTEGA, R., ***El Estado vigilante***, Tecnos, Madrid, 2000, p. 195.

[29] GÓMEZ PUENTE, M., ***La inactividad de la Administración***, 2.ª ed., Aranzadi, Elcano, 2000, pp. 93-94.

necesario publicar (o, al menos, estar disponibles conforme a las leyes de transparencia) qué tipo de datos, en general, se suministraron a la herramienta informática para tomar la decisión. En la mayoría de casos, esto será suficiente para asegurar que el resultado final dado por el ***big data*** no estará basado en criterios discriminatorios.

Por el contrario, no parece que deba incluirse en esa publicidad/transparencia ni el código del algoritmo utilizado para tomar las decisiones ni tampoco debería ser obligatorio que se publicite el resultado final dado por la herramienta[30]. Esto es, ni las empresas ni las personas físicas tendrán derecho a conocer las probabilidades de incumplir que le asigna la herramienta.

La justificación es triple. De un lado, informar a las empresas de que tienen una baja probabilidad de ser investigadas podría incrementar el propio incumplimiento. De otro lado, publicar el código o las ponderaciones realizadas por la herramienta para tomar la decisión permitiría –a las empresas que pudieran pagar un servicio informático de suficiente nivel– revelar la misma información respecto a las posibilidades concretas de ser inspeccionadas. Por último, esa información en manos de las empresas les permitiría modificar su comportamiento para alterar los resultados del algoritmo. Es decir, si la empresa sabe qué variable, en qué proporción y de qué forma inciden en la probabilidad de ser investigadas, esta podría alterar su comportamiento no para cumplir, sino para modificar esas variables (lo que se ha llamado *gaming the algorithm*)[31].

Por esta razón, a pesar de la necesidad de asegurar la transparencia y la falta de arbitrariedad o discriminación, no parece posible exigir que se revele toda la información respecto a la herramienta informática ni cómo esta toma sus decisiones con objeto de evitar que las empresas o sujetos infractores puedan usar esa información para seguir incumpliendo la norma. Por otro lado, sí parece exigible que la Administración revele qué tipo de datos son usados por el algoritmo para tomar su decisión con objeto de asegurar que no se está utilizando información protegida (art. 9 RGPD) o discriminatoria (art. 14 CE). Por último, dada la posibilidad de que el ***big data*** pueda inferir informaciones discriminatorias basadas en datos no discriminatorios (ej., deducir la raza o nacionalidad basándose en el barrio dónde se vive), con objeto de evitar que esto ocurra, parece necesario que el algoritmo, no publicado, supere algún tipo de auditoría administrativa interna –o de un tercero– que verifique que el algoritmo por su propia cuenta no está "descubriendo" datos prohibidos o sensibles y usándolos en sus resultados[32].

---

30 Incluso aquella parte de la doctrina que más fervientemente apoya la publicación de toda la información respecto a la herramienta o algoritmo utilizado por la Administración pública sostiene que, en el caso de los algoritmos que deciden el campo de actuación de una inspección, la transparencia debe tener límites. BOIX PALOP, A., "Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones", cit., p. 265.

31 BAMBUER, J. y ZARSKY, T., "The algorithm game", ***Notre Dame Law Review***, n. 94 (1), 2018.

32 GONZÁLEZ ESPEJO, M.J., "Sector público y algoritmos: Transparencia o un poco más de paciencia", ***Diario la Ley***, Wolters Kluwer, 19 de febrero de 2020. Disponible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAyNDEyMTNTK0stKs7Mz7M1MjACCVqq5eWnpla4ONuW5qWkpmXmpaaAlGSmVbrkJ4dUFqTapiXmFKeqpSbl52ejmBQPMwEAZnEi5GMAAAA=WKE.

## 4 *Big data* como método de selección de la inspección en la jurisprudencia comparada: Francia y Holanda

La cuestión que se acaba de analizar, sobre la validez de estos sistemas y el nivel de transparencia requerida, ha sido enjuiciada en alguno de los países de nuestro alrededor con resultados dispares.

Así, el Consejo Constitucional francés, en su Decisión de 27 de diciembre de 2019 (Decisión n. 2019-796 DC), examina la validez de un sistema de uso del ***big data*** para apoyar la selección de objetivos de la Inspección de Hacienda. El sistema fue incorporado a través de la Ley de presupuestos de 2020 (art. 154), permitiendo a las autoridades tributarias que usaran estas herramientas con dos finalidades: la primera, recolectar datos públicos que existan en internet sobre los obligados tributarios; en segundo lugar, procesar de forma automatizada esa información para decidir si existen posibles fraudes.

De esta forma, la autorización legislativa no se limita al procesamiento de los datos que ya tiene la Inspección para decidir el riesgo de incumplimiento, sino que adicionalmente permite que la herramienta se use para escanear internet en búsqueda de indicios de fraude –por ejemplo, página web de una empresa que vende productos, pero no paga tributos, etc.–.

La Corte Constitucional, en su fallo, admite el uso de ambas funcionalidades automatizadas de la herramienta, principalmente con base en los siguientes argumentos: i) la finalidad es un objetivo constitucionalmente protegido (lucha contra el fraude) y se aplica en un ámbito donde pueden producirse incumplimientos de la norma no detectados por los medios ordinarios; ii) los datos incorporados a la herramienta y los resultados obtenidos solamente pueden ser usados por personal de la Administración sujeta al secreto profesional y confidencialidad; iii) los indicios de fraude captados de forma automatizada a través de algoritmos no sirven como prueba única para fundamentar una sanción, sino que esta solamente podrá ser resultado de procedimientos debidamente individualizados y motivados con los derechos de defensa (audiencia) y garantías habituales.

En cualquier caso, la Corte advierte que este es un examen preliminar y que la validez de la herramienta dependerá de que, en su uso, esta permita un control de legalidad y de que los derechos y garantías fundamentales de los ciudadanos queden asegurados.

Por otro lado, mucho más restrictiva y contundente se muestra la Sentencia del Tribunal de distrito de La Haya (***Rechtbank Den Haag***) en los Países Bajos, de fecha 5 de febrero de 2020 (ECLI:NL: RBDHA: 2020:865), que declara ilícito el uso de un algoritmo para establecer probabilidades de incumplimiento de ciudadanos que perciben prestaciones de la Seguridad Social[33].

[33] Ver BATTAGLINI MANRIQUE DE LARA, M., "Sentencia histórica del Tribunal de la Haya anulando la elaboración de perfiles para el fraude de la Seguridad Social (SyRI)", ***World Compliance Association***, 2020. Disponible en: http://www.worldcomplianceassociation.com/2624/noticia-sentencia-historica-del-tribunal-de-la-haya-anulando-la-elaboracion-de-perfiles-para-el-fraude-de-la-seguridad-social-syri.html; COTINO HUESO, L., "«SyRI, ¿a quién sanciono?» Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020", ***La***

La sentencia responde a la demanda de varias asociaciones de defensa de los derechos humanos que impugnan el uso por parte de la Inspección de Trabajo y Seguridad Social del denominado Sistema de Indicación de Riesgos (***Systeem Risico Indicatie***, SyRI). Esta es una herramienta automatizada que el Gobierno holandés usa para prevenir y combatir el fraude en el campo de la Seguridad Social[34].

El sistema, a través de un instrumento informático automatizado, asigna un nivel de riesgo de que una persona cometa fraude a partir de una serie de parámetros estudiados y correlacionados entre sí. La herramienta viene autorizada por la Ley de organización de implementación y estructura de ingresos (***Wet structuur uitvoeringsorganisatie en inkomen***, SUWI). Esta norma (art. 65.2) permite la elaboración de informes de riesgos para evaluar las posibilidades de que una persona física o jurídica cometa fraude en la percepción de prestaciones públicas incluidas en materia de Seguridad Social. El Gobierno justifica este uso debido al elevado número de fraude detectado en el país.

Dicha ley está desarrollada en un reglamento que fija los datos procesados por la herramienta de ***big data***. Concretamente, se procesa información como la siguiente: nombre, dirección, lugar de residencia, dirección postal, fecha de nacimiento, género y características administrativas de las personas; datos respecto a su trabajo; sanciones administrativas anteriores; datos fiscales, incluida información sobre bienes muebles e inmuebles; datos sobre motivos de exclusión de asistencia o beneficios; datos comerciales; datos de integración, que son datos que pueden usarse para determinar si se han impuesto obligaciones de integración a una persona; historial de cumplimiento de las leyes y reglamentos; datos sobre becas recibidas; sobre pensiones; sobre la obligación de reintegro de prestaciones públicas; sobre endeudamiento; sobre beneficios, ayudas y subsidios recibidos; sobre permisos y exenciones recibidos para la realización de actividades y datos sobre si tiene o no seguro de salud.

El análisis de los datos y la evaluación del riesgo se realiza en dos tramos. En primer lugar, los datos se hacen anónimos a través del reemplazo del nombre personal y los números de la Seguridad Social por un código. Posteriormente, se comparan los datos con el modelo de riesgos y se identifican los posibles factores de riesgo. Si a una persona se le otorga un grado alto de riesgo de fraude, sus datos son trasvasados a la segunda parte del proceso. En esta segunda parte, el análisis de riesgo lo realiza una unidad específica dentro de la Inspección de Trabajo (Inspección de Asuntos Sociales y Empleo), que le asigna un riesgo definitivo.

Ante este sistema, el tribunal holandés considera que la normativa viola el artículo 8.2 del CEDH al entender que la injerencia en la vida privada de las personas de este sistema de análisis de riesgo no cumple el requisito de necesidad ni proporcionalidad. En este sentido, la sentencia estima que, a pesar de reconocer que la medida persigue

*Ley Privacidad*, n. 4, 2020; FERNÁNDEZ, C.B., "Primera sentencia europea que declara ilegal un algoritmo de evaluación de características personales de los ciudadanos", *Diario la Ley*, 13 de febrero de 2020. Disponible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAyNDa3NDJUK0stKs7Mz7M1MjACC6rl5aekhrg425bmpaSmZealpoCUZKZVuuQnh1QWpNqmJeYUp6qlJuXnZ6OYFA8zAQCfSdkrYwAAAA==WKE.

[34] ALGORITHMWATCH y BERTELSMANN STIFTUNG, *Automating Society taking stock of automated decisión making in the EU*, Berlín, 2019, p. 101.

una finalidad legítima (lucha contra el fraude), la intromisión en la vida privada no está suficientemente justificada. A su vez, el tribunal establece que, aunque el informe de riesgos generado por el algoritmo no tiene en sí mismo una consecuencia legal directa (no hay sanción), sí que tiene un efecto significativo en la vida privada de la persona a la que se refiere.

Así, la sentencia concluye que la herramienta informática, en aplicación del derecho de la Unión –RGPD y CEDH–, no cumple con los principios de transparencia, de limitación del tratamiento y de minimización de datos, concluyendo que la normativa que regula el uso de la aplicación es insuficientemente clara y verificable, lo que la convierte en contraria a la ley.

La sentencia incide especialmente en la falta de transparencia. En este sentido, el tribunal indica que esa falta de transparencia plantea problemas de comprobación de posibles efectos discriminatorios (indirectos); sobre todo, añade la sentencia, dado que el análisis de riesgo de incumplimiento se realiza sobre sujetos en situaciones de especial vulnerabilidad –por esa razón acceden en primer lugar a las prestaciones sociales–. Además, el tribunal recrimina que el sistema analice datos personales de categorías especiales (art. 9 RGPD), y advierte de la posibilidad de que el algoritmo, realizando conexiones e inferencias, acabe tomando decisiones discriminatorias[35]. En este sentido, establece que, sobre la base de la información existente acerca de la herramienta, no es posible evaluar si ese riesgo de discriminación indirecta ha sido abordado adecuadamente por la norma que desarrolla el sistema de evaluación de riesgos.

En mi opinión, esta sentencia tiene varias lecturas. Por un lado, si entendemos que las conclusiones obtenidas en ella son aplicables y extensibles a cualquier uso de un algoritmo para valorar riesgos de fraude, muy probablemente sus conclusiones llevan a una prohibición ***de facto*** de sus posibilidades de uso. Es cierto que la sentencia no llega a prohibir su implantación, pero los requisitos que establece pueden hacer imposible el mismo.

Téngase en cuenta que la sentencia analiza un sistema de por sí bastante garantista con la protección de datos y la intimidad. En este sentido, los datos estaban anonimizados, se establecía una obligación de borrado de datos a los cuatro meses si el informe indicaba riesgo bajo, se compartimentaba las secciones y departamentos que procesaban información, se obligaba a la confidencialidad y, además, en última instancia era la Inspección la que tomaba la última decisión[36]. Además, la utilización



[35] Esto ha sido puesto de relieve por la doctrina en varias ocasiones al entender que esta tecnología parece capaz de inferir ciertas características personales basadas en otros datos. Es decir, aunque se prohíba recabar datos en materia de afiliación sindical, religión, sexo, orientación sexual o discapacidad, los algoritmos son capaces de obtener esta información a través de otros datos (CRAWFORD, K. y SCHULTZ, J., "Big data and due process: Towards a framework to redress predictive privacy harms", cit.). Por ejemplo, la religión o la raza pueden estar estadísticamente muy relacionadas con el código postal o el barrio donde vive la persona. Así pues, tomar decisiones basadas en la ubicación de la vivienda resultará en el fondo una decisión basada en la raza o, incluso, conforme al tiempo dedicado a leer unas noticias en Facebook o Google –y no otras– se puede predecir la afiliación política o sindical. De hecho, en muchos casos, se desconocen las capacidades de un algoritmo a la hora de hacer inferencias estadísticas, lo que supone la "imposibilidad" de conocer si el propio algoritmo está tomando decisiones fundamentadas en información discriminatoria o no, en HARDT, M., "How big data is unfair", ***Medium***, 26 de septiembre de 2014. Disponible en: https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de.

[36] Si bien es cierto que no se sabe si la Inspección finalmente decidía inspeccionar todos los sujetos con riesgo alto –sin tomar ninguna decisión significativa– o, por el contrario, si esta intervención humana era relevante para la decisión final, una

del sistema no era indiscriminada, sino que, por el contrario, era necesario solicitar su uso –para poder hacerlo había unos requisitos específicos fijados y la norma establecía quién podía solicitar el informe de riesgo–, qué datos debían usarse y con qué finalidad –objetivo específico–. A pesar de todo ello, el tribunal entiende que no existen garantías adecuadas, dado que "no hay información suficiente para saber cómo operaba". Incide posteriormente la sentencia en esta cuestión al criticar que el modelo de riesgo que se utiliza y los indicadores de riesgo sean secretos y que eso impide que un sujeto interesado pueda defenderse contra el hecho de que se haya determinado un alto riesgo de fraude sobre él o ella.

En esta cuestión es donde, de aceptar esta lectura de la sentencia, se vendría a prohibir ***de facto*** el uso de este tipo de herramientas automatizadas para valorar riesgos de incumplimiento. En efecto, si se da información suficiente para saber cómo opera la herramienta –como parece exigir la sentencia comentada–, esta será inservible para sus propios objetivos. Por un lado, aquellos que tuvieran un bajo riesgo y lo supieran[37] tendrían incentivos para incumplir conociendo que las probabilidades de ser investigados son bajas. Por otro lado, los que tuvieran un alto riesgo de ser inspeccionados y conocieran "cómo opera el algoritmo" podrían modificar su conducta, no para cumplir, sino para engañar al sistema de valoración de riesgo –una posibilidad que la doctrina ha puesto de manifiesto en varias ocasiones–[38]. En fin, en mi opinión, la transparencia en el funcionamiento del sistema de valoración de riesgos de fraude no puede ser tal que permita a los sujetos evadir la vigilancia y el control.

También es cierto que la sentencia apunta hacia otras posibilidades, dado que el tribunal señala expresamente que echa en falta una revisión previa por parte de la Administración o de un tercero independiente de que el algoritmo es proporcionado, vistos los derechos en juego y que, adicionalmente, no es discriminatorio. Esta posibilidad parece más sensata. Es decir, dada la imposibilidad de una transparencia absoluta para que el sistema sea efectivo –lo que ***de facto*** limita las posibilidades de defensa de los ciudadanos–, tendría sentido aceptar que la propia Administración o un tercero independiente auditara el algoritmo para asegurar que funciona correctamente y sin sesgos.

Además, la sentencia parece olvidar que la decisión automatizada –de ser realmente automatizada, porque parece existir suficiente intervención humana cuando el informe de riesgos se envía a la Inspección de Trabajo– solamente tiene como efecto que se inicie una investigación –es un mero selector–, siendo la investigación la que determinará si hay sanción o no. Con esto no quiero decir que la selección de los sujetos a investigar no tenga efectos sobre las personas, pero, en cualquier caso, las consecuencias no son absolutas ni irrevocables. A este respecto, solamente señalo que la sentencia parece olvidar poner en proporción las garantías necesarias para poder

cuestión que podría ser relevante para justificar que la decisión final no era tomada por el algoritmo automáticamente.

37 Que no se informe a los sujetos de que tienen un bajo riesgo es uno de los reproches "indirectos" que hace la sentencia a la configuración del sistema.

38 BOIX PALOP, A., "Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones", cit., p. 48; BAMBUER, J. y ZARSKY, T., "The algorithm game", cit., p. 46.

tomar decisiones basadas en un algoritmo, con los efectos que dicha decisión produce[39]. Es decir, no sería proporcionado exigir las mismas garantías para un algoritmo que adjudica riesgo de reincidencia de un delincuente cuya consecuencia sea ampliar el número de años en prisión [Sentencia State ***v.*** Loomis, 881, N.W.2d 749, 7532 (Wis, 2016)] que las garantías necesarias para un algoritmo que da apoyo a la Inspección para decidir qué sujeto comenzar a auditar, siendo el posterior análisis e investigación realizados completamente por personas conforme al procedimiento habitual.

En cualquier caso, como se ha dicho, en mi opinión, esta sentencia tiene otra lectura muy distinta a la anterior. Se debe partir de que esta sentencia responde a un tipo de herramienta con finalidades muy concretas que puede haber llevado al tribunal a buscar unos estándares de exigencia tan altos que ***de facto*** acabe prohibiéndola. Las razones son las siguientes: en primer lugar, afecta a personas físicas. Ninguno de los argumentos vistos en ella parece aplicable a empresas, las cuales no disfrutan del derecho a la protección de datos ni tampoco una investigación puede ser considerada una invasión de la vida privada de esta, por cuanto una empresa no tiene vida privada como derecho fundamental.

En segundo lugar, y esta podría ser la clave de bóveda de la sentencia, la detección del fraude en materia de prestaciones a la Seguridad Social afecta a colectivos especialmente vulnerables que podrían merecer una mayor protección –mayores garantías– de su vida privada. Como establecieron los demandantes, y el relator especial de la ONU, este sistema "tiene un efecto discriminatorio y estigmatizador", dado que se centra en investigar vecindarios más marginados y, con ello, "contribuye a los estereotipos y refuerza una imagen negativa de los ocupantes de dichos vecindarios". Hablamos de personas con incapacidades permanentes, invalidez o en desempleo: ciudadanos que, de una forma u otra, son especialmente vulnerables, por lo que desarrollar una herramienta de máxima tecnología para detectar fraude entre ellos puede considerarse una "criminalización de la pobreza".

De hecho, como sostienen los expertos, la mayor parte del fraude en Seguridad Social no proviene por el cobro de prestaciones indebidas, sino por la falta de pago de las cotizaciones y por la economía informal[40]. De esta forma, usar medidas invasivas de la privacidad de las personas sin, a su vez, utilizar las mismas medidas para atacar las mayores fuentes de fraude podría entenderse, en efecto, arbitrario, injustificado o, al menos, desproporcionado.

Téngase en cuenta que, desde el momento en que derechos fundamentales de los ciudadanos entran en juego –especialmente en colectivos socialmente vulnerables–, ya no debe actuar libremente el principio de discrecionalidad administrativa, sino que este vendrá limitado por los principios de necesidad y proporcionalidad. De esta forma, intentar justificar dicha medida invasiva de los derechos fundamentales de las personas por la necesidad de evitar el fraude –necesidad legítima en abstracto– cuando no se está atacando fuentes de fraude mayores –economía informal,

[39] COTINO HUESO, L., "Derecho y garantías ante el uso público y privado de inteligencia artificial, robótica y ***big data***", cit.

[40] UPIT, ***Estudio sobre el estado y actividad de la ITSS***, Madrid, 2014. Disponible en: http://upit.es/web/index/show/id/36 (Consultado el 6 de abril de 2020).

infracotización, etc.– y que, además, no requerirían de la invasión de derechos de las personas (dado que estos ilícitos son realizados por empresas) puede considerarse contrario a estos principios.

Por estas razones, no creo que la doctrina de esta sentencia deba entenderse como un impedimento general y abstracto al uso del ***big data*** o de los procesos automatizados para dar soporte a las decisiones de selección de sujetos infractores. Más bien parece que la sentencia puede estar oponiéndose a una política de "criminalización de la pobreza" respecto a un gobierno enfocando sus esfuerzos –uso de la máxima tecnología disponible– para detectar el pequeño fraude de personas en general en situaciones vulnerables, a la vez que poco se hace en la misma línea por la lucha contra el gran fraude (violando los principios de necesidad y proporcionalidad con ello).

En fin, pocas dudas caben de la necesidad de garantizar los derechos fundamentales de las personas frente al Estado y, en especial, evitar sesgos discriminatorios. Al mismo tiempo, poco sentido tendría limitar las posibilidades de adaptación de las administraciones al siglo XXI permitiendo usar sus recursos más eficientemente, a la vez que consiguen recompensar mejor a los sujetos cumplidores a través de una menor probabilidad de ser objeto de una inspección. De esta forma, la ley debe preocuparse especialmente de que el sistema funcione –que las razones de elección no respondan a sesgos o discriminaciones, sino a una verdadera mayor probabilidad de infringir la norma– y que exista suficiente transparencia para que el sistema pueda ser enjuiciado en caso de presentar indicios de arbitrariedad o de discriminación.

## 5 Síntesis de los retos legales en la implantación del *big data* como método de selección de sujetos a investigar y algunas recomendaciones

A pesar de que la selección de uno u otro sujeto, para iniciar una inspección, está configurada jurídicamente como una decisión discrecional de la Administración, el uso de herramientas automatizadas para la construcción de perfiles de riesgo de incumplimiento de la normativa presenta múltiples conflictos jurídicos, especialmente en materia de protección de datos, protección de la intimidad y posibles discriminaciones. De esta forma, la Administración, en el diseño de la herramienta informática, deberá tener en cuenta estos derechos y establecer garantías que protejan los derechos fundamentales de los ciudadanos.

La intensidad de esas garantías es una cuestión actualmente muy debatida por la doctrina y los tribunales, sin que exista consenso. No obstante, sí se pueden fijar una serie de pautas a seguir.

En primer lugar, se deberá valorar la necesidad del uso de la herramienta, entendida como la existencia de un objetivo legítimo –en este caso la lucha contra el fraude–. No obstante, no parece suficiente una justificación abstracta de la necesidad de alcanzar ese objetivo, sino concretamente de la relación entre la consecución de ese objetivo y el uso de la herramienta automatizada (adecuación). De esta forma, como se ha visto en este trabajo, podría entenderse que, si se quiere perseguir el fraude –finalidad

legítima en abstracto–, no debería utilizarse una herramienta automática de selección de perfiles contra pequeños defraudadores si no se usa para grandes defraudadores –que sería la forma de alcanzar verdaderamente el objetivo–.

En segundo lugar, la proporcionalidad. En efecto, las garantías para salvaguardar los derechos de los ciudadanos deben ser proporcionadas respecto al daño que la herramienta informática puede generar. De esta forma, no será lo mismo una herramienta que establezca perfiles de riesgo de reincidencia cuyo uso puede implicar el alargamiento de una pena privativa de libertad que las garantías que debe tener un sistema que establece un riesgo de cometer una infracción laboral cuya única posible consecuencia es el inicio de una investigación, la cual será la que determine, en última instancia, si existió o no ilícito.

En tercer lugar, no será lo mismo una herramienta informática que se limite a procesar datos que ya obran en poder de la Administración pública que otra que se dedique a escanear internet con objeto de recolectar datos para la vigilancia y control de la normativa. En efecto, las posibilidades tecnológicas son múltiples y no todas tienen la misma repercusión. De esta forma, se deberán exigir mayores garantías a una herramienta que recopila datos sin consentimiento de los interesados que a otra que solamente los procesa con objeto de ayudar a tomar decisiones acertadas respecto a la selección de sujetos que se van a investigar.

En cuarto lugar, la cuestión más compleja de resolver será la necesidad de transparencia. Pocas dudas caben de que, para garantizar el derecho de defensa del afectado y para evitar discriminaciones directas o indirectas, es imprescindible que el proceso de selección sea transparente. No obstante, a pesar de que esto sea así, cuando el algoritmo tiene por objetivo, concretamente, la lucha contra el fraude, la transparencia –más bien el exceso de ella– puede dejar inoperativa la propia herramienta.

En efecto, la información respecto a cómo funciona el algoritmo puede desvelar información clave que, de un lado, incremente el incumplimiento y, de otro lado, permita a un incumplidor reducir el riesgo de ser detectado. Por esta razón, aunque se comparta la necesidad de la "transparencia algorítmica", parece recomendable buscar otras fórmulas que no frustren los resultados deseados. En este trabajo se exponen dos: i) publicar qué datos se suministran a la herramienta para tomar sus decisiones, ya que esto eliminaría las posibilidades de que se utilicen datos sensibles o discriminatorios: ii) otra posibilidad podría ser que, internamente o a través de un organismo especializado independiente, se realizara un análisis de verificabilidad de la herramienta informática que comprobara que no se usan datos prohibidos y que los resultados no son discriminatorios.

Por último, se debe señalar que la protección, las garantías y las salvaguardas frente a la herramienta no tienen por qué ser las mismas si el informe sobre probabilidad de incumplir la normativa se hace respecto de una empresa que si se hace sobre una persona física. Por ello, parece recomendable para la Administración establecer dos sistemas diferenciados de selección, para que, de esta forma, además de poder fijar estándares de garantía distintos en caso de que se quiera, en el supuesto de que se

impugnara el sistema –y ante una eventual anulación o prohibición de uso del mismo–, el tribunal pudiera valorar por separado la licitud de cada uno.

# 6 Conclusiones: ventajas y límites del uso del *big data* en la inspección

## 6.1 Beneficios aportados

El uso de las herramientas del ***big data*** y la inteligencia artificial permite la planificación estratégica y la selección de sujetos a inspeccionar para mejorar el uso de los recursos de la Inspección[41]. Estos mecanismos son capaces de clasificar a cada empresa basada en su riesgo de incumplimiento[42]. De esta forma, extrayendo información y patrones ocultos, se mejora la ratio de acierto, encontrando más incumplimientos, a la vez que se reducen las inspecciones en empresas que cumplen. En particular, el ***big data*** proporciona las siguientes ventajas al sistema:

1. Se reduce el tiempo y los recursos dedicados al análisis manual de datos.

2. Se permite una rápida curva de aprendizaje de los nuevos inspectores sin que sean necesarios años de experiencia para desarrollar intuiciones sobre dónde buscar los incumplimientos.

3. Se localizan patrones y tendencias de incumplimiento indetectables por la intuición a través de la correlación de datos.

4. Permite la planificación de campañas de forma más eficiente.

5. Proporciona la posibilidad de detectar y atajar las llamadas "epidemias" de fraude antes de que se expandan.

6. La selección basada en datos incrementa una visión medioplacista o largoplacista de los objetivos. Esto reduce las posibilidades de tomar decisiones "a golpe de telediario". Esto es, decisiones basadas en sucesos puntuales que modifican el curso de la acción inspectora por la relevancia momentánea de un hecho y no porque existan verdaderas razones justificativas de tal actuación[43].

7. Las técnicas del ***big data*** también mejoran la evaluación de la actuación inspectora en términos generales. De un lado, permite definir el nivel de incumplimiento en un país o sector y cómo este disminuye gracias a las actuaciones de la Administración. Ello incrementará la legitimidad social de la necesidad de la Inspección, basándose en datos en un mundo en el que aquello que no puede medirse pocas veces se tiene en cuenta.

8. Estas técnicas de tratamiento de datos también facilitan su propia evaluación para mejorar cada día a través del ***feedback*** de los inspectores.

---

41 WATKINS, R.C., REYNOLDS, K.M., DEMARA, R., GEORGIOPOULOS, M., GONZÁLEZ, A. y EAGLIN, R., "Exploring Data mining technologies as tools to investigate money laundering", *Journal of Policing practice and research: An international Journal*, n. 4(2), 2013, p. 12.

42 OECD, *Best Practice Principles for Regulatory Policy Regulatory Enforcement and Inspections*, OECD Press, París, 2014, p. 28.

43 OCDE, *OECD Regulatory Enforcement and Inspections Toolkit*, cit., p. 29.

En fin, cada vez más países adoptan estas técnicas para mejorar la selección de sujetos a inspeccionar con notable éxito. Austria, tras la inclusión de estas técnicas basadas en riesgos de incumplimiento para la selección, pasó de encontrar entre 20 y 30 fraudes por cada 100 inspecciones realizadas a descubrir incumplimientos de entre el 60 y el 80% de las inspecciones efectuadas[44]. Adicionalmente, este sistema permitió también incrementar el cumplimiento voluntario a través de las comunicaciones (cartas), avisando de la información que se tenía. La previa selección permitió que el cumplimiento pasara de producirse en un 7% de los que recibían la carta a un 20 o 30%[45].

## 6.2 Límites en el uso del *big data*

A pesar de las oportunidades que brinda la aplicación de estas modernas técnicas para mejorar la efectividad de las inspecciones, su incorporación exige tener los datos con calidad suficiente y una apuesta segura por estos. Todo ello no siempre es posible o sencillo.

1. En primer lugar, el ***big data*** necesita nutrirse de suficientes datos de calidad para poder obtener conclusiones válidas. Esto implica juntar todos los datos en una misma herramienta informática con la colaboración de otras administraciones (CC. AA) y otras ramas de la Administración estatal (Hacienda, DGT, etc.,). En este sentido, en nuestro país se han hecho muchos avances, pero se debe recordar que cuantos más datos se tengan mayor fiabilidad existirá[46].

2. Adicionalmente a tener los datos, estos no deben estar sesgados o incompletos. Por ejemplo, si en el pasado se ha focalizado en un determinado tipo de empresas –donde lógicamente se habrán encontrado incumplimientos– y esos son los datos que se suministran a la herramienta, basándose en esos datos se considerará que estas empresas son las que deben ser inspeccionadas en el futuro. Esto, a su vez, implicará mayor número de fraudes encontrados en esas empresas, confirmando el sesgo y cerrando el círculo[47]. Por esta razón, es tan importante que los datos suministrados sean completos, de calidad y sin sesgos manifiestos.

3. También será necesario dar formación a los inspectores sobre la utilidad de la herramienta y cómo usarla, además de proporcionarles formación para que sean capaces de dar ***feedback*** a la misma[48].

4. Otra cuestión que puede limitar el uso de la herramienta es la desconfianza a lo nuevo. Toda organización suele sentirse más cómoda haciendo las cosas como sabe



[44] En ambos casos, el índice de acierto en la selección era mejor que seleccionar de manera aleatoria, cuyo índice era del 15-20%.

[45] OCDE, *Compliance Risk Management: Audit Case Selection Systems*, OECD Press, París, 2004, p. 40.

[46] OCDE, *OECD Regulatory Enforcement and Inspections Toolkit*, cit., p. 39.

[47] RIDEMAR, A., *Decision Support for SWEA Inspections*, Kth Royal Institute of Technology School of Electrical Engineering and Computer Science, Stockholm, 2018, p. 33. Disponible en: https://kth.diva-portal.org/smash/get/diva2:1238767/FULLTEXT01.pdf (Consultado el 6 de abril de 2020).

[48] WATKINS, R.C., REYNOLDS, K.M., DEMARA, R., GEORGIOPOULOS, M., GONZÁLEZ, A. y EAGLIN, R., "Exploring Data mining technologies as tools to investigate money laundering", cit., p. 12.

hacerlas, y la inclusión de nuevos mecanismos provoca rechazo. Por esta razón, es importante que se conozca el funcionamiento y las mecánicas subyacentes a la herramienta, de tal forma que se genere confianza en su uso[49].

5. Se debe señalar que el ***big data*** no objetiviza el uso de los recursos, solamente hace más eficiente esa utilización. Por esta razón, seguirá siendo necesaria la incorporación de los conocimientos y experiencias de los inspectores, así como la reflexión y la toma de decisiones sobre priorización. El sistema de ***big data*** en ningún caso sustituye la necesidad de una planificación estratégica ni elimina el uso de la discrecionalidad administrativa para elegir objetivos. El ***big data*** es una herramienta que ayuda a esa toma de decisiones y a elegir esos objetivos.

6. Por último, estas herramientas pueden acabar siendo usadas para justificar la persecución de ciertos colectivos históricamente discriminados. Sobre todo en materia de policía, se ha criticado que se usen estas herramientas para justificar una mayor vigilancia en los barrios pobres o la detención en aeropuertos de personas de color[50]. En efecto, en este trabajo se ha puesto de manifiesto el peligro de que los mecanismos se utilicen para justificar un uso de los recursos enfocados en investigar más a pequeñas empresas o a receptores de prestaciones. Por ello, estos sistemas de selección requieren una constante vigilancia y crítica como cualquier otro de los existentes.

En este sentido, será necesario establecer controles internos y externos para asegurar que los derechos fundamentales de las personas no son violados. De un lado, la Administración tiene la obligación de que la selección no responda a patrones discriminatorios –ni voluntarios (suministrando datos protegidos) ni involuntarios (suministrando datos que por error están sesgados)–. De otro lado, es necesario que la selección y el uso de la herramienta sean transparentes. Por supuesto, esto no puede implicar la obligación para la Administración de publicar el resultado del análisis de riesgo –bajo la amenaza de que ello se utilice para infringir la norma–, sino que se debe publicar qué datos son tenidos en cuenta, de forma general, por el ***big data*** para crear el índice de riesgo.

## Bibliografía

ALGORITHMWATCH y BERTELSMANN STIFTUNG, ***Automating Society taking stock of automated decision making in the EU***, Berlín, 2019.

ALLINGHAM, M.G. y SANDMO, A., "Income Tax Evasion: A Theoretical Analysis", ***Journal of Public Economics***, n. 1, 1972.

BAMBUER, J. y ZARSKY, T., "The algorithm game", ***Notre Dame Law Review***, n. 94(1), 2018.

BATTAGLINI MANRIQUE DE LARA, M., "Sentencia histórica del Tribunal de la Haya anulando la elaboración de perfiles para el fraude de la Seguridad Social (SyRI)",

[49] WATKINS, R.C., REYNOLDS, K.M., DEMARA, R., GEORGIOPOULOS, M., GONZÁLEZ, A. y EAGLIN, R., "Exploring Data mining technologies as tools to investigate money laundering", cit., p. 12.

[50] GILL, P., ***Rounding up the usual suspects?: developments in contemporary law enforcement intelligence***, Ashgate, Aldershot, 2020; SANDERS, C.B. y SHEPTYCKI, J., "Policing, crime and big data: towards a critique of moral economy of stochastic governance", ***Crime Law Soc Change***, n. 68, 2017, p. 7.

*World Compliance Association*, 2020. Disponible en: http://www.worldcomplianceassociation.com/2624/noticia-sentencia-historica-del-tribunal-de-la-haya-anulando-la-elaboracion-de-perfiles-para-el-fraude-de-la-seguridad-social-syri.html.

BECKER, G., "Crime and Punishment: An Economic Approach", *Journal of Political Economy*, n. 76(2), 1968.

BERMEJO VERA, J., "La Administración inspectora", *Revista de Administración Pública*, n. 147, 1998.

BOIX PALOP, A., "Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones", *Revista de Derecho Público: Teoría y Método*, n. 1, 2020.

BONCHI, F., GIANNOTTI, F., MAINETTO, G. y PEDRESCHI, D., "A classification-based methodology for planning audit strategies in fraud detection", *KDD '99: Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining*, 1999. Disponible en: https://dl.acm.org/doi/10.1145/312129.312224 (Consultado el 6 de abril de 2020).

CERRILLO I MARTÍNEZ, A., "El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?", *Revista General de Derecho Administrativo*, n. 50, 2019.

COMISIÓN EUROPEA, *Risk Management Guide for Tax Administrations,* Bruselas, 2006. Disponible en: https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/taxation/tax_cooperation/gen_overview/risk_management_guide_for_tax_administrations_en.pdf.

COMISIÓN EUROPEA, *Libro Blanco. Sobre la Inteligencia Artificial - Un enfoque europeo para la excelencia y la confianza,* COM (2020) 65 final, Bruselas, 2020.

COTINO HUESO, L., "Derecho y garantías ante el uso público y privado de inteligencia artificial, robótica y *big data*", Bauzá Reilly, M. (dir.), *El Derecho de las Tics en Latinoamérica*, La Ley, Uruguay, 2019.

COTINO HUESO, L., "Riesgos e impactos del *big data*, la inteligencia artificial y la robótica. Enfoques, modelos y principios de la respuesta del derecho", *Revista General de Derecho Administrativo*, n. 50, 2019.

COTINO HUESO, L., "«SyRI, ¿a quién sanciono?» Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020", *La Ley Privacidad*, n. 4, 2020.

CRAWFORD, K. y SCHULTZ, J., "*Big data* and due process: Towards a framework to redress predictive privacy harms", *Boston College Law Review*, n. 55 (1), 2014.

FERNÁNDEZ, C.B., "Primera sentencia europea que declara ilegal un algoritmo de evaluación de características personales de los ciudadanos", *Diario la Ley*, 13 de febrero de 2020. Disponible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAyNDa3NDJUK0stKs7Mz7M1MjACC6rl5aekhrg425bmpaSmZealpoCUZKZVuuQnh1QWpNqmJeYUp6qlJuXnZ6OYFA8zAQCfSdkrYwAAAA==WKE.

FREEMAN, K., "Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State *v.* Loomis", ***North Carolina Journal of Law & Technology***, n. 18, 2016.

GILL, P., ***Rounding up the usual suspects?: developments in contemporary law enforcement intelligence***, Ashgate, Aldershot, 2020.

GÓMEZ PUENTE, M., ***La inactividad de la Administración***, 2.ª ed., Aranzadi, Elcano, 2000.

GONZÁLEZ ESPEJO, M.J., "Sector público y algoritmos: Transparencia o un poco más de paciencia", ***Diario la Ley***, Wolters Kluwer, 19 de febrero de 2020. Disponible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAyNDEyMTNTK0stKs7Mz7M1MjACCVqq5eWnpIa4ONuW5qWkpmXmpaaAlGSmVbrkJ4dUFqTapiXmFKeqpSbl52ejmBQPMwEAZnEi5GMAAAA=WKE.

GT29, ***Guidelines on Automated individual decisión-making and Profiling for the purposes of Regulation 2016/679***, 2016 (Adoptadas el 3 de octubre de 2017).

GUPTA, M. y NAGADEVARA, V., "Audit Selection Strategy for Improving Tax Compliance – Application of Data Mining Techniques", ***Foundations of E-Government – Conference Proceedings, 11th International Conference on e-Governance***, Hyderabad, India, 2007.

HARDT, M., "How ***big data*** is unfair", ***Medium***, 26 de septiembre de 2014. Disponible en: https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de.

MARTÍNEZ GARAY, L., "Peligrosidad, algoritmos y ***due process***: el caso State ***vs.*** Loomis", ***Revista de Derecho penal y criminología***, n. 20, 2018.

OCDE, ***Compliance Risk Management: Audit Case Selection Systems***, OECD Press, París, 2004.

OCDE, ***Best Practice Principles for Regulatory Policy Regulatory Enforcement and Inspections***, OECD Press, París, 2014.

OCDE, ***OECD Regulatory Enforcement and Inspections Toolkit***, OECD Press, París, 2018.

PONCE SOLÉ, J., "Inteligencia artificial, derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", ***Revista General de Derecho Administrativo***, n. 50, 2019.

REBOLLO PUIG, M., "La actividad inspectora", Díez Sánchez, J.J. (coord.), ***Actas del VIII Congreso de la Asociación Española de Profesores de Derecho Administrativo: La función inspectora***, INAP, Madrid, 2013.

RIDEMAR, A., ***Decision Support for SWEA Inspections***, Kth Royal Institute of Technology School of Electrical Engineering and Computer Science, Stockholm, 2018. Disponible en: https://kth.diva-portal.org/smash/get/diva2:1238767/FULLTEXT01.pdf (Consultado el 6 de abril de 2020).

RIVERO ORTEGA, R., ***El Estado vigilante***, Tecnos, Madrid, 2000.

SANDERS, C.B. y SHEPTYCKI, J., "Policing, crime and ***big data***: towards a critique of moral economy of stochastic governance", ***Crime Law Soc Change***, n. 68, 2017.

SRINIVASAN, T.N., "Tax Evasion: A model", ***Journal of Public Economics***, n. 2, issue 4, 1973.

TODOLÍ SIGNES, A., "La gobernanza colectiva de la protección de datos en las relaciones laborales: ***big data***, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos", ***Revista de Derecho Social***, n. 84, 2018.

UPIT, ***Estudio sobre el estado y actividad de la ITSS***, Madrid, 2014. Disponible en: http://upit.es/web/index/show/id/36 (Consultado el 6 de abril de 2020).

WATKINS, R.C., REYNOLDS, K.M., DEMARA, R., GEORGIOPOULOS, M., GONZÁLEZ, A. y EAGLIN, R., "Exploring Data mining technologies as tools to investigate money laundering", ***Journal of Policing practice and research: An international Journal***, n. 4(2), 2013.

YITZHAKI, S., "Income tax evasion: A theoretical analysis", ***Journal of Public Economics***, n. 3, issue 2, 1974.