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 axudante doutor de Dereito do Traballo e da Seguridade Social
Universidade 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 trasparencia de la Administración, la llamada "trasparencia algorítmica". Sin embargo, como se discute en este trabajo, dicha trasparencia 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, trasparencia 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 A selección de suxeitos obxecto dunha investigación

O dereito do traballo e da seguridade social parte, como presuposto habilitante da súa propia existencia, dun desequilibrio de poder entre as partes suxeitas a este. Isto non soamente ten efectos en materia de negociación de condicións de traballo, senón tamén nas posibilidades da parte débil de exixir o cumprimento dos seus dereitos. Por esta razón, a construción de ordenamento social, desde as súas orixes, veu acompañado da necesidade dunha vixilancia e control de carácter público do seu cumprimento. Isto realizouse e realízase, principalmente, a través da Inspección de Traballo e da Seguridade Social.

Actualmente existen diferentes fórmulas para conseguir o cumprimento da norma por parte dos obrigados; non obstante, a realización de indagacións e a proposta de

sancións en caso de descubrir un incumprimento seguen a ser as principais ferramentas con que conta o Estado para facer cumprir as súas normas[1].

Un exitoso programa de inspeccións non ten como consecuencia soamente os efectos directos en cada acción individual (en termos de conseguir o cumprimento do inspeccionado, por exemplo, a recadación obtida desa inspección). Pola contra, existen outros efectos indirectos, en moitos sentidos máis relevantes, para o mantemento xeral do nivel de cumprimento das normas[2].

En efecto, a existencia dun sistema eficiente de control que localice e castigue os que infrinxen a norma convencerá o resto de obrigados que cumprila redunda no seu beneficio[3]. Pola súa vez, incrementará a percepción de poder ser inspeccionado, algo que, de acordo co modelo estándar de cumprimento das normas, conducirá a un incremento do cumprimento voluntario[4]. Por último, un sistema de inspección que audite e castigue os que contraveñen a norma porá fin á competencia desleal entre as empresas, eliminando unha posible necesidade de incumprir para poder competir no mercado en igualdade de condicións.

Non obstante, a ninguén lle escapa que o proceso de inspección é un proceso intrusivo non moi benvido polas empresas[5]. Mesmo para as empresas que non infrinxen ningunha normativa, e non reciben ningún requirimento nin sanción, a presenza da Inspección nas súas instalacións e a solicitude de información é unha intromisión que altera a normal convivencia dentro desta. Sumado ao anterior, as inspeccións son un procedemento custoso, tanto en capital humano como financeiro para o Estado[6].

A Inspección debe, por esta razón, usar os seus limitados recursos de xeito prudente para obter o máximo nivel de cumprimento coa mínima intrusión e os mínimos custos[7]. Planear axeitadamente unha estratexia de inspeccións é clave para detectar a fraude ***a posteriori***, así como para proactivamente previr que existan incumprimentos da norma. É dicir, partindo da hipótese de que inspeccionar unha empresa que cumpre coa norma proporciona poucos beneficios á prevención da fraude, a selección dos suxeitos obxecto da inspección será esencial. O obxectivo, pois, será planificar

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. e 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. e SANDMO, A., "Income Tax Evasion: A Theoretical Analysis", *Journal of Public Economics*, n. 1, 1972, pp. 323-338.

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

6 BONCHI, F., GIANNOTTI, F., MAINETTO, G. e 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. Dispoñible en: https://dl.acm.org/doi/10.1145/312129.312224 (Consultado o 6 de abril de 2020).

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

estratexicamente a actuación inspectora de tal forma que cada inspección se realice sobre unha empresa que incumpra.

Neste sentido, parece que hai campo para a mellora nalgúns sectores. De acordo co Informe anual 2018 da Inspección de Traballo e Seguridade Social, en materia de contratación de traballadores, a actividade planificada ofreceu os seguintes resultados. Dun total de 55.640 actuacións, detectouse a comisión de 3.877 infraccións sancionables. Iso significa que o "acerto", á hora de seleccionar as empresas obxecto da inspección durante unha campaña dirixida, foi do 6%[8] aproximadamente. Respecto ao tempo de traballo, realizáronse 20.465 actuacións cun resultado de 5.230 infraccións[9], o que implica un éxito do 25%.

En xeral, en materia de emprego e relacións laborais, incluíndo non só a actividade planificada, senón tamén aquela realizada como resposta a unha denuncia, o nivel de acerto á hora de realizar unha inspección que rematase na detección dun incumprimento sancionable foi do 12%[10]. Iso implica, en sentido contrario, que se usaron recursos da Inspección e se alterou o normal funcionamento dunha empresa nun 88% dos casos, sen que ese comportamento viñese xustificado pola gravidade do incumprimento desta[11].

Por outra banda, existe outro fenómeno que merece atención específica. En materia de prevención de riscos laborais no sector da construción, do total de 28.134 ordes de servizo, a suma de requirimentos e infraccións –aquí a memoria da Inspección non dá datos desagregados– foi de 32.345. Iso significa un acerto do 114% na actuación. Este non é un fenómeno específico da construción, dado que o acerto no resto de sectores se sitúa no 126%. Isto é, ***grosso modo*** e en termos xerais, en cada empresa visitada detectáronse de media 1,26 incumprimentos. Estes datos amosan conclusións preocupantes.

Dun lado, podería implicar un grande acerto por parte da Inspección de Traballo á hora de seleccionar que empresas son auditadas en materia de prevención de riscos. No entanto, sen información ningunha que faga pensar que existe un xeito distinto de seleccionar as empresas inspeccionadas nesta materia das anteriores que se acaban de ver, probablemente máis ben supoña un incumprimento sistemático nesta materia. Non obstante, iso non significa que a planificación estratéxica resulte innecesaria nesta materia, senón que o obxectivo da planificación en materia de prevención debería

8 Iso supondo que cada infracción foi a unha única empresa, sendo posible tamén que as sancións por contratación fraudulenta de traballadores temporais se concentrasen nunhas poucas empresas, o que reduciría aínda máis o nivel de acerto. Por outro lado, a memoria tamén recolle un total de 21.199 requirimentos. Iso significa, probablemente, que se atoparon irregularidades nesas empresas, aínda que de insuficiente relevancia como para seren sancionadas. Contando tamén cos requirimentos, o nivel de "acerto" situaríase no 45%.

9 Igualmente, neste caso, poderíanse engadir os 6.040 requirimentos que se realizaron nesta materia, dando un resultado de acerto neste caso do 55%.

10 Tendo en conta os requirimentos, o nivel de éxito sería do 40%.

11 Todo iso aos ollos da propia Inspección de Traballo e da Seguridade Social, que, tras iniciar a inspección, decidiu non sancionar. Por suposto, tamén é posible que a decisión final de non sancionar viñese causada non porque non exista incumprimento que mereza ser sancionado, senón pola falta de probas que o acrediten. Non obstante, este argumento non resta razóns ao aquí sustentado. Se a Inspección audita unha empresa e finalmente non atopa probas suficientes para sancionar, non se terá producido o efecto indirecto en termos de prevención xeral tan necesario nestas actuacións e no uso de recursos.

ser distinto. Neste sentido, non se debería pretender atopar algún incumprimento, do tipo que sexa, por cada inspección, senón seleccionar as empresas que realizan os incumprimentos máis graves.

En efecto, a planificación estratéxica debe pretender sempre maximizar os resultados da actuación inspectora[12]. Por isto, na planificación, o obxectivo será decidir auditar aquelas empresas onde existe un risco maior dun incumprimento ***grave***. En materia de prevención de riscos laborais, esta diferenciación é sinxela de observar. Non será o mesmo, á hora de decidir auditar unha empresa ou outra, que unha incumpra unha normativa que implique un alto risco de accidente mortal que outra que implique riscos menores. Non se pon en dúbida a necesidade de auditar todas as empresas incumpridoras. Non obstante, sendo os recursos escasos, pode ter sentido priorizar estratexicamente a redución dos accidentes máis graves.

Por esta razón, nos últimos anos impulsouse, desde moitas administracións[13], o uso de tecnoloxías da información –***big data***, ***data mining***, ***machine learning***, algoritmos, intelixencia artificial, etc.– co obxecto de mellorar a selección das empresas a inspeccionar ou de obxectivos das campañas, baseándose no procesamento automatizado dos datos.

Este traballo ten como obxectivo discutir os beneficios e limitacións do uso da tecnoloxía do ***big data*** como forma de tomar decisións respecto a que empresas inspeccionar en materia de traballo e seguridade social. Para iso, na epígrafe 2 analizaranse os distintos modelos de selección de empresas obxecto desta inspección. A terceira epígrafe dedicarase ás mecánicas de funcionamento do sistema de valoración da fraude. A cuarta, á necesidade de avaliar os resultados. A quinta considera os retos legais en materia de protección de datos, intimidade e regulación antidiscriminatoria da implantación do sistema. O traballo remata concluíndo coas vantaxes e límites desta tecnoloxía en materia de prevención da fraude.

2 Retos legais: protección de datos e dereitos fundamentais afectados

O uso de algoritmos, a clasificación dos suxeitos mediante perfís de risco de incumprimento e o tratamento de datos de forma automatizada a través das técnicas descritas neste traballo co obxecto de seleccionar as empresas que cómpre inspeccionar pode formular múltiples problemas xurídicos. Por unha banda, as normas de protección de datos e, pola outra, as normas antidiscriminación e de protección da intimidade poden supor límites xurídicos ao uso destas técnicas.

A análise particularizada da legalidade do emprego destas técnicas dificilmente pode facerse neste momento de forma abstracta e ***a priori*** sen coñecer exactamente

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

[13] COMISIÓN EUROPEA, ***Risk Management Guide for Tax Administrations,*** Bruxelas, 2006. Dispoñible 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.

as mecánicas e o tipo de información que o sistema utiliza. Por iso, esta epígrafe limítase a sinalar os retos xurídicos que pode presentar este uso e os principios legais que deben orientar a adopción destas técnicas por parte da Inspección. Para efectuar esta análise, primeiro débese dividir a cuestión entre os suxeitos afectados: dun lado, o uso do ***big data*** para seleccionar persoas xurídicas ou empresas e, doutro, para seleccionar profesionais autónomos ou persoas individuais.

2.1 Aplicación do *big data* para seleccionar persoas xurídicas ou empresas

A necesaria segmentación respecto á selección de persoas xurídicas fronte á selección de persoas físicas parte da propia división realizada pola normativa. En efecto, o RXPD circunscríbese á protección de ***datos persoais***, incluíndo soamente os datos das persoas físicas e excluíndo do seu ámbito de aplicación os datos das persoas xurídicas (art. 1 e 2 RXPD)[14].

Deste xeito, o tratamento automatizado de datos das empresas e o seu procesamento a través de técnicas de ***big data*** non vén protexido por esta normativa[15]. Serán os principios xerais, a obriga da Administración de rexerse baixo o principio de legalidade, de igualdade de trato e a prohibición de arbitrariedade os que determinarán as súas posibilidades de uso. Iso leva a que, no emprego do ***big data*** para a selección de empresas a investigar, á falta de normativa específica en materia de protección de datos, se apliquen os controis clásicos e habituais na Administración.

2.2 Aplicación para a selección de persoas físicas ou autónomos

En materia de vixilancia do cumprimento da normativa social, a Inspección tamén é a encargada de controlar a posible fraude de prestacións sociais recibidas por persoas físicas e o cumprimento da normativa laboral por parte de profesionais autónomos respecto á Seguridade Social propia e en canto á súa posición como empregador.

2.2.1 Protección de datos e autónomos

Unha primeira cuestión que xorde é se a normativa en materia de protección de datos persoais se aplica aos autónomos e profesionais no exercicio da súa profesión. A este respecto xorden dúbidas dado que, a pesar de que son persoas físicas, interactúan como empresarios no mercado. Esta cuestión foi tratada pola doutrina xudicial e chegou á conclusión de que se entende que soamente están excluídos do ámbito de

[14] Expresamente, o artigo 4 define «datos persoais» como "toda información sobre unha persoa física identificada ou identificable («o interesado»); considerarase persoa física identificable toda persoa cuxa identidade poida determinarse".

[15] Non obstante, téñase en conta que os datos da empresa ou da actividade empresarial quedarán excluídos da aplicación desta normativa, pero non os datos dos profesionais e traballadores (persoa física) que se atopen integrados na organización; ver Informe xurídico AEPD 2008/0371.

aplicación da normativa de protección de datos aqueles profesionais que exercen a súa actividade baixo a forma de persoa xurídica[16].

En efecto, a Sentenza da Audiencia Nacional do 21 de novembro de 2002 (rec. 881/2000) considera que a publicación dos datos identificativos dos arquitectos está protexida pola LOPD, posto que son datos que "se *refiren a profesionais que non exercen a súa actividade baixo forma de empresa, non tendo en consecuencia a condición de comerciante á cal se refiren os artigos primeiro e seguintes do Código de comercio*".

No mesmo sentido, a SAN do 11 de febreiro de 2004 (rec. 119/2002) sinala que "*no caso examinado o dato do afectado, aínda que se refira ao lugar de exercicio da súa profesión é un dato dunha persoa física cunha actividade profesional cuxa protección cae na órbita da Lei orgánica 15/1999*".

Tamén o Tribunal Supremo –Sala 3.ª– en Sentenza do 20 de febreiro de 2007 (rec. 732/2003) é do mesmo parecer ao establecer que "*Está claro que os arquitectos e promotores a que se refire o litixio participan da natureza de persoas físicas e que non deixan de selo pola súa condición de profesionais ou axentes que interveñen no mercado da construción, polo que os datos persoais relativos a estes quedan amparados e suxeitos en canto ao seu tratamento informatizado ás previsións da LORTAD; e é que desde este punto de vista subxectivo a exclusión do ámbito de aplicación da LORTAD non vén determinado polo carácter profesional ou non do afectado ou titular dos datos obxecto de tratamento, senón pola natureza de persoa física ou xurídica titular dos datos, en canto só as persoas físicas se consideran titulares dos dereitos a que se refire o artigo 18.4 da Constitución*".

Desta forma, os datos profesionais dos traballadores autónomos –en canto son persoas físicas– estarán amparados pola normativa en materia de protección de datos persoais vixente.

3 Límites xurídicos á aplicación do *big data* na loita contra a fraude laboral

3.1 Decisións automatizadas e protección de datos

Aclarado que a normativa en materia de protección de datos será aplicable tanto a profesionais autónomos como a persoas físicas –perceptores de prestacións sociais–, vaise agora analizar o réxime xurídico aplicable.

O RXPD, no seu artigo 6.1 e), establece que o tratamento de datos das persoas físicas é lícito se "é necesario para o cumprimento dunha misión realizada en interese público ou no exercicio de poderes públicos conferidos ao responsable do tratamento". Así pois, co amparo da Lei 23/2015, do 21 de xullo, ordenadora do Sistema de Inspección de Traballo e Seguridade Social –concretamente o seu artigo 18.2 e 18.4 –, a recollida e tratamento destes datos será lícita.

[16] AEPD R/00598/2007.

Adicionalmente, aínda que a recollida de datos e o seu tratamento sexan lícitos conforme se acaba de ver, o artigo 22 do RXPD fixa unha regra específica para a toma de decisións baseadas unicamente neste tratamento automatizado ou na elaboración de perfís. En concreto, este artigo prohibe[17] que unha decisión final, que teña efectos xurídicos sobre o suxeito[18], estea baseada unicamente nese tratamento automatizado ou perfil elaborado polo algoritmo sen intervención humana. Isto pode afectar de cheo ás posibilidades de seleccionar automatizadamente (ou mediante perfís de persoas físicas ou autónomos) os suxeitos a inspeccionar.

Non obstante, esta prohibición aplícase só se non existe ningún tipo de intervención humana na selección final do suxeito obxecto da inspección. En efecto, o artigo 22 RXPD que aquí se analiza soamente prohibe a "decisión baseada ***unicamente*** no tratamento automatizado". Por esta razón, se existe intervención humana ***significativa*** na toma de decisión, non será de aplicación esta imposibilidade[19].

Neste sentido, nos casos en que a decisión final queda en mans do inspector, cuxa decisión será tomada conforme a súa experiencia usando unicamente o índice de risco de incumprimento como un factor a ter en conta, non parece que nos atopemos no suposto prohibido do artigo 22 RXPD. Da mesma forma, se os plans estratéxicos e as campañas son decididos polos responsables da Inspección, tampouco parece que se estivese ante este suposto[20].

En calquera caso, unha vez máis, o artigo 22 RXPD establece excepcións á súa aplicación. O regulamento permite que se elaboren decisións totalmente automatizadas, sempre que iso veña autorizado polo dereito nacional (art. 22.1 b RXPD). Así, o artigo 16.3 da Lei 23/2015 considera a posibilidade de que a Inspección reciba datos cedidos pola Axencia Tributaria e a Seguridade Social, incluíndo os datos persoais obxecto de tratamento automatizado. Esta parece unha habilitación suficiente tendo en conta que a cesión de datos sempre é un exercicio máis intenso que o mero tratamento; así pois, poderíase soster que quen pode o máis pode o menos (se se permite legalmente a cesión dos datos, permítese o seu tratamento automatizado). Porén, en caso de que se desexe poder seleccionar os suxeitos obxecto da inspección sen intervención

---

17 Literalmente, o artigo 22 RXPD non establece unha prohibición, senón que a regra se configura como "o dereito a non ser obxecto deste tipo de decisións". Non obstante, como xa se discutiu e argumentou noutro 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 dereito debe entenderse como unha prohibición tal como o interpreta o GT29, ***Guidelines on Automated individual decisión-making and Profiling for the purposes of Regulation 2016***/679, 2016 (adoptadas o 3 de outubro de 2017), p. 13. Isto é, configúrase como unha prohibición –sen necesidade de reclamar activamente o dereito– aos responsables de datos de tomar as decisións con esta metodoloxía automatizada.

18 Na miña opinión, non parece que haxa dúbidas de que abrir unha inspección sobre unha persoa física ou un autónomo ten efectos xurídicos (ex., obriga de responder solicitudes de información, etc.), polo que este criterio estaría cumprido.

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 calquera caso, recórdese que a intervención humana na toma de decisión debe ser significativa. Estase ante un concepto xurídico indeterminado en que se deberá analizar caso a caso o nivel de intervención. O que está claro é que, se os responsables da Inspección se limitan a validar a decisión tomada polo ***big data*** en todas as ocasións, podería non haber intervención suficiente para excluír estas proteccións. Neste sentido, para saber se o nivel de intervención humana é "significativo", haberá que valorar con que frecuencia o responsable de recursos humanos adopta decisións finais nun sentido distinto ao formulado polo algoritmo ou a 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.

humana ningunha, sería recomendable unha actualización da normativa nacional que expresamente aclarase a posibilidade do tratamento automatizado e a elaboración de perfís con este obxectivo e establecese garantías suficientes de transparencia e antidiscriminación.

3.2 Garantías fronte á toma de decisións automatizada

A Comisión Europea, no seu ***Libro branco sobre intelixencia artificial***[21] alerta dunha serie de perigos existente no uso da IA, entre os que se atopa a opacidade dalgúns destes sistemas de ***big data***, decisións algorítmicas discriminatorias contra colectivos protexidos ou decisións erróneas por un mal deseño dos algoritmos[22]. Co obxecto de evitar estes prexuízos, a Comisión Europea (2020) sostén a necesidade de establecer garantías a favor dos afectados por un sistema de intelixencia artificial.

A regulación proposta parte de que non todos os sistemas teñen a mesma incidencia sobre eses dereitos fundamentais; por iso, formúlase un sistema de garantías distinto dependendo do risco que teña a IA de afectar a eses dereitos fundamentais. Desta forma, podería haber ata cinco niveis baseados no risco de que unha intelixencia artificial afecte ou vulnere dereitos fundamentais. Isto é, dependendo dos seus potenciais efectos, requiriría desde a ausencia de garantías no caso dos sistemas de IA máis inocuos ata a prohibición absoluta no caso dos sistemas de intelixencia artificial máis perigosos.

En efecto, a doutrina vén sinalando desde hai tempo a posibilidade de que os sistemas de decisión automatizada conculquen dereitos fundamentais e a necesidade de garantías no seu uso[23]. Neste sentido, pode indicarse como exemplo o uso por parte dos EE. UU. dun algoritmo para determinar a probabilidade de reincidencia dun suxeito que cometeu un delito. Neste caso, os xuíces utilizan esa probabilidade para determinar a duración das penas privativas de liberdade. Dado que a metodoloxía e o algoritmo usados para a avaliación do risco de reincidencia son descoñecidos para o defendido, alegouse violación do dereito de defensa e ao proceso debido dada a imposibilidade de impugnar esa valoración do risco nin de saber se esa valoración estaba nesgada ou era directamente discriminatoria (especialmente contra persoas de cor nos EE. UU.).

Non obstante, o Tribunal Supremo do estado de Wisconsin na Sentenza State ***v.*** Loomis[24] considerou que o feito de que o acusado non soubese a metodoloxía da avaliación do risco usada polo algoritmo non viola o seu dereito a un proceso debido nin a

[21] COMISIÓN EUROPEA, ***Libro branco sobre a intelixencia artificial - Un enfoque europeo para a excelencia e a confianza,*** COM (2020) 65 final, Bruxelas, 2020.

[22] No mesmo sentido pronúncianse 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. e SCHULTZ, J., "Big data and due process: Towards a framework to redress predictive privacy harms", ***Boston College Law Review***, n. 55 (1), 2014.

[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 o 17 de xullo de 2018).

unha sentenza individualizada, dado que o informe soamente é un máis dos factores tidos en conta polo xuíz para fixar a sentenza definitiva. Ademais, neste caso, sostense que non é posible entregar a información sobre o funcionamento do algoritmo nin a metodoloxía usada, posto que é un "segredo de empresa" (os informes son contratados pola Administración de xustiza a unha empresa privada).

Ante estas conclusións, a doutrina criticou a sentenza e sostivo a necesidade de que exista total transparencia na metodoloxía empregada polo algoritmo co obxecto de poder impugnar o informe e coñecer se esta estaba a usar criterios discriminatorios para realizar a valoración final do risco de reincidencia (ex., cor de pel)[25]. En efecto, débese estar de acordo con estas críticas, e é que, cando a liberdade de circulación dunha persoa está en xogo, a liberdade de empresa ou o segredo empresarial non pode ser argumentación suficiente para permitir unha opacidade que impida coñecer posibles discriminacións.

Por esta razón, o RXPD sinala que, mesmo cando unha lei nacional autorice o uso de mecanismos informáticos para tomar decisións automatizadas, será necesario que esta mesma normativa fixe controis e salvagardas dos dereitos e liberdades dos suxeitos afectados. Non obstante, conforme o criterio mantido pola Comisión Europea[26] na súa cualificación dos tipos de algoritmos segundo as súas consecuencias, parece claro que esas garantías deberán ser proporcionais aos efectos, máis ou menos intensos, que as decisións automatizadas teñan sobre o suxeito.

3.3 Discrecionalidade administrativa na elección de suxeitos a investigar e garantías fronte á arbitrariedade ou discriminación

A elección do suxeito a investigar, así como a orientación mediante plans de inspección desta, cualifícanse xuridicamente de actos discrecionais[27]. Deste xeito, o inspector poderá elixir, baseándose na súa experiencia –como se fai tradicionalmente–, ou noutros datos ou informacións, os suxeitos obxecto do seu traballo. Da mesma forma, a confección de plans estratéxicos e operativos desde os mandos xerárquicos da inspección só vén elevar esa potestade discrecional a instancias superiores. Neste sentido, admítese pacificamente a inclusión neles de criterios de oportunidade e o establecemento de prioridades e estratexias para aplicar coa máxima eficiencia recursos limitados desta[28].

Ata aquí non parece que exista límite legal ningún para o uso do ***big data*** como soporte para a toma das ditas decisións. Non obstante, non está de máis recordar que

---

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 branco sobre a intelixencia artificial - Un enfoque europeo para a excelencia e a 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.

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

a discrecionalidade non pode significar arbitrariedade e que ten límites, co obxecto de evitar abusos e discriminacións[29]. Así, da mesma forma que na elección dos suxeitos a inspeccionar non sería lícito realizala baseándose exclusivamente na nacionalidade da empresa ou da persoa física, tampouco o ***big data*** podería levarnos a esa conclusión –nin sequera de forma indirecta– sen que existan razóns obxectivas distintas ao criterio discriminatorio que o xustifique.

Así pois, débese partir de que, ***a priori***, non existe diferente réxime xurídico aplicable cando a decisión é tomada fundamentándose na experiencia do inspector, nos datos existentes, en criterios de oportunidade ou no ***big data***. Isto é, o importante non reside na forma ou procedemento elixido para tomar a decisión, senón en comprobar que o resultado desta –a decisión– non sexa arbitrario ou discriminatorio.

O problema radica nas posibilidades de defensa do suxeito investigado. En efecto, nun caso ou outro, o suxeito seleccionado descoñecerá as razóns polas que saíu elixido, o que fará materialmente imposible demostrar en xuízo un trato nesgado ou discriminatorio da Inspección. Por esta razón, o artigo 20.2 da Lei 23/2015 establece que cómpre garantir a efectividade dos principios de igualdade de trato e non discriminación no exercicio da actividade inspectora. Ou sexa, é a Administración a obrigada a asegurarse de que as decisións non se toman en contra do principio de igualdade. Pola súa vez, este artigo garante a publicación das instrucións de organización de servizos, dos criterios operativos xerais e dos criterios técnicos vinculantes.

Desta forma, dun lado, a Administración ten a obriga de asegurar que o ***big data*** non estea a dar como resultado unha elección discriminatoria ou sen fundamento suficiente; por outro lado, será necesario garantir certo grao de transparencia nos criterios utilizados polo ***big data*** para tomar as súas decisións e establecer as porcentaxes de risco de incumprimento de cada empresa ou dos distintos sectores.

Isto é, non parece que sexa suficiente indicar que se elixiu unha empresa –ou un sector se falamos dun plan estratéxico– porque a ferramenta informática indica que ten maior risco de incumprir. Pola contra, a Administración terá a obriga de asegurar que o resultado final do índice de risco de incumprimentos non está baseado en criterios prohibidos (nacionalidade da empresa ou persoa física, sindicación ou non, etc.). A analoxía coas ferramentas de selección tradicionais ata o momento é sinxela, e é que, segundo o principio de igualdade, a Administración tamén debe asegurarse de que un inspector non actúe motivado por razóns arbitrarias e discriminatorias.

Deste xeito, igual que, de acordo coa normativa actual, os criterios operativos xerais deben ser publicados para garantir a non arbitrariedade, parece necesario publicar (ou, polo menos, estar dispoñibles conforme as leis de transparencia) que tipo de datos, en xeral, se lle subministraron á ferramenta informática para tomar a decisión. Na maioría de casos, isto será suficiente para asegurar que o resultado final dado polo ***big data*** non estará baseado en criterios discriminatorios.

Pola contra, non parece que deba incluírse nesa publicidade/transparencia nin o código do algoritmo utilizado para tomar as decisións nin tampouco debería ser

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

obrigatorio que se publicite o resultado final dado pola ferramenta[30]. Isto é, nin as empresas nin as persoas físicas terán dereito a coñecer as probabilidades de incumprir que lle asigna a ferramenta.

A xustificación é tripla. Por unha banda, informar as empresas de que teñen unha baixa probabilidade de ser investigadas podería incrementar o propio incumprimento. Por outra parte, publicar o código ou as ponderacións realizadas pola ferramenta para tomar a decisión permitiría –ás empresas que puidesen pagar un servizo informático de suficiente nivel– revelar a mesma información respecto ás posibilidades concretas de ser inspeccionadas. Por último, esa información en mans das empresas permitiríalles modificar o seu comportamento para alterar os resultados do algoritmo. É dicir, se a empresa sabe que variable, en que proporción e de que forma inciden na probabilidade de ser investigadas, esta podería alterar o seu comportamento non para cumprir, senón para modificar esas variables (o que se chamou ***gaming the algorithm***)[31].

Por esta razón, malia a necesidade de asegurar a transparencia e a falta de arbitrariedade ou discriminación, non parece posible exixir que se revele toda a información respecto á ferramenta informática nin como esta toma as súas decisións co obxecto de evitar que as empresas ou suxeitos infractores poidan usar esa información para seguir incumprindo a norma. Por outro lado, si parece exixible que a Administración revele que tipo de datos son usados polo algoritmo para tomar a súa decisión co obxecto de asegurar que non se está a utilizar información protexida (art. 9 RXPD) ou discriminatoria (art. 14 CE). Por último, dada a posibilidade de que o ***big data*** poida inferir informacións discriminatorias baseadas en datos non discriminatorios (ex., deducir a raza ou nacionalidade baseándose no barrio onde se vive), co obxecto de evitar que isto suceda, parece necesario que o algoritmo, non publicado, supere algún tipo de auditoría administrativa interna –ou dun terceiro– que verifique que o algoritmo pola súa propia conta "non está a descubrir" datos prohibidos ou sensibles e usándoos nos seus resultados[32].

4 *Big data* como método de selección da inspección na xurisprudencia comparada: Francia e Holanda

A cuestión que se acaba de analizar, sobre a validez destes sistemas e o nivel de transparencia requirida, foi axuizada nalgún dos países do noso arredor con resultados dispares.

30 Mesmo aquela parte da doutrina que máis ferventemente apoia a publicación de toda a información respecto á ferramenta ou algoritmo utilizado pola Administración pública sostén que, no caso dos algoritmos que deciden o campo de actuación dunha inspección, a transparencia debe ter 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. e 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 febreiro de 2020. Dispoñible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAyNDEyMTNTK0stKs7Mz7M1MjACCVqq5eWnpla4ONuW5qWkpmXmpaaAlGSmVbrkJ4dUFqTapiXmFKeqpSbl52ejmBQPMwEAZnEi5GMAAAA=WKE.

Así, o Consello Constitucional francés, na súa Decisión do 27 de decembro de 2019 (Decisión n. 2019-796 DC), examina a validez dun sistema de uso do ***big data*** para apoiar a selección de obxectivos da Inspección de Facenda. O sistema foi incorporado a través da Lei de orzamentos de 2020 (art. 154), permitindo ás autoridades tributarias que usasen estas ferramentas con dúas finalidades: a primeira, reunir datos públicos que existan en Internet sobre os obrigados tributarios; en segundo lugar, procesar de forma automatizada esa información para decidir se existen posibles fraudes.

Deste xeito, a autorización lexislativa non se limita ao procesamento dos datos que xa ten a Inspección para decidir o risco de incumprimento, senón que adicionalmente permite que a ferramenta se empregue para escanear Internet en busca de indicios de fraude –por exemplo, páxina web dunha empresa que vende produtos, pero non paga tributos, etc.–.

A Corte Constitucional, na súa resolución, admite o uso das dúas funcionalidades automatizadas da ferramenta, principalmente con base nos seguintes argumentos: i) a finalidade é un obxectivo constitucionalmente protexido (loita contra a fraude) e aplícase nun ámbito onde poden producirse incumprimentos da norma non detectados polos medios ordinarios; ii) os datos incorporados á ferramenta e os resultados obtidos só poden ser usados por persoal da Administración suxeita ao segredo profesional e confidencialidade; iii) os indicios de fraude captados de forma automatizada a través de algoritmos non serven como proba única para fundamentar unha sanción, senón que esta soamente poderá ser resultado de procedementos debidamente individualizados e motivados cos dereitos de defensa (audiencia) e garantías habituais.

En calquera caso, a Corte advirte que este é un exame preliminar e que a validez da ferramenta dependerá de que, no seu uso, esta permita un control de legalidade e de que os dereitos e garantías fundamentais dos cidadáns queden asegurados.

Por outro lado, moito máis restritiva e contundente se mostra a Sentenza do Tribunal de distrito da Haia (***Rechtbank Dean Haag***) nos Países Baixos, do 5 de febreiro de 2020 (ECLI:NL: RBDHA: 2020:865), que declara ilícito o uso dun algoritmo para establecer probabilidades de incumprimento de cidadáns que perciben prestacións da Seguridade Social[33].

A sentenza responde á demanda de varias asociacións de defensa dos dereitos humanos que impugnan o uso por parte da Inspección de Traballo e Seguridade Social do denominado Sistema de Indicación de Riscos (***Systeem Risico Indicatie***, SyRI). Esta é unha ferramenta automatizada que o Goberno holandés usa para previr e combater a fraude no campo da Seguridade Social[34].

[33] 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. Dispoñible 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 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 febreiro de 2020. Dispoñible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbH1czUwMDAyNDa3NDJUK0stKs7Mz7M1MjACC6rl5aekhrg425bmpaSmZealpoCUZKZVuuQnh1QWpNqmJeYUp6qlJuXnZ6OYFA8zAQCfSdkrYwAAAA==WKE.

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

O sistema, a través dun instrumento informático automatizado, asigna un nivel de risco de que unha persoa cometa fraude a partir dunha serie de parámetros estudados e correlacionados entre si. A ferramenta vén autorizada pola Lei de organización de implementación e estrutura de ingresos (***Wet structuur uitvoeringsorganisatie en inkomen***, SUWI). Esta norma (art. 65.2) permite a elaboración de informes de riscos para avaliar as posibilidades de que unha persoa física ou xurídica cometa fraude na percepción de prestacións públicas incluídas en materia de Seguridade Social. O Goberno xustifica este uso debido ao elevado número de fraude detectada no país.

A devandita lei está desenvolvida nun regulamento que fixa os datos procesados pola ferramenta de ***big data***. Concretamente, procésase información como a seguinte: nome, enderezo, lugar de residencia, enderezo postal, data de nacemento, xénero e características administrativas das persoas; datos respecto ao seu traballo; sancións administrativas anteriores; datos fiscais, incluída información sobre bens mobles e inmobles; datos sobre motivos de exclusión de asistencia ou beneficios; datos comerciais; datos de integración, que son datos que poden usarse para determinar se se lle impuxeron obrigas de integración a unha persoa; historial de cumprimento das leis e regulamentos; datos sobre bolsas recibidas; sobre pensións; sobre a obriga de reintegro de prestacións públicas; sobre endebedamento; sobre beneficios, axudas e subsidios recibidos; sobre permisos e exencións recibidos para a realización de actividades e datos sobre se ten ou non seguro de saúde.

A análise dos datos e a avaliación do risco realízase en dous tramos. En primeiro lugar, os datos fanse anónimos a través da substitución do nome persoal e os números da Seguridade Social por un código. Posteriormente, compáranse os datos co modelo de riscos e identifícanse os posibles factores de risco. Se a unha persoa se lle outorga un grao alto de risco de fraude, os seus datos son transvasados á segunda parte do proceso. Nesta segunda parte, a análise de risco realízao unha unidade específica dentro da Inspección de Traballo (Inspección de Asuntos Sociais e Emprego), que lle asigna un risco definitivo.

Ante este sistema, o tribunal holandés considera que a normativa viola o artigo 8.2 do CEDH ao entender que a inxerencia na vida privada das persoas deste sistema de análise de risco non cumpre o requisito de necesidade nin proporcionalidade. Neste sentido, a sentenza estima que, a pesar de recoñecer que a medida persegue unha finalidade lexítima (loita contra a fraude), a intromisión na vida privada non está suficientemente xustificada. Pola súa vez, o tribunal establece que, malia que o informe de riscos xerado polo algoritmo non ten en si mesmo unha consecuencia legal directa (non hai sanción), si que ten un efecto significativo na vida privada da persoa á cal se refire.

Así, a sentenza conclúe que a ferramenta informática, en aplicación do dereito da Unión –RXPD e CEDH–, non cumpre cos principios de transparencia, de limitación do tratamento e de minimización de datos, concluíndo que a normativa que regula o uso da aplicación é insuficientemente clara e verificable, o que a converte en contraria á lei.

A sentenza incide especialmente na falta de transparencia. Neste sentido, o tribunal indica que esa falta de transparencia presenta problemas de comprobación de

posibles efectos discriminatorios (indirectos); sobre todo, engade a sentenza, dado que a análise de risco de incumprimento se realiza sobre suxeitos en situacións de especial vulnerabilidade –por esa razón acceden en primeiro lugar ás prestacións sociais–. Ademais, o tribunal recrimina que o sistema analice datos persoais de categorías especiais (art. 9 RXPD), e advirte da posibilidade de que o algoritmo, realizando conexións e inferencias, acabe tomando decisións discriminatorias[35]. Neste sentido, establece que, sobre a base da información existente acerca da ferramenta, non é posible avaliar se ese risco de discriminación indirecta foi abordado axeitadamente pola norma que desenvolve o sistema de avaliación de riscos.

Na miña opinión, esta sentenza ten varias lecturas. Por un lado, se entendemos que as conclusións obtidas nela son aplicables e extensibles a calquera uso dun algoritmo para valorar riscos de fraude, moi probablemente as súas conclusións levan a unha prohibición ***de facto*** das súas posibilidades de uso. É certo que a sentenza non chega a prohibir a súa implantación, pero os requisitos que establece poden facer imposible este.

Téñase en conta que a sentenza analiza un sistema de por si bastante garantista coa protección de datos e a intimidade. Neste sentido, os datos estaban anonimizados, establecíase unha obriga de borrado de datos aos catro meses se o informe indicaba risco baixo, compartimentábanse as seccións e departamentos que procesaban información, obrigábase á confidencialidade e, ademais, en última instancia era a Inspección a que tomaba a última decisión[36]. Ademais, o emprego do sistema non era indiscriminado, senón que, pola contra, cumpría solicitar o seu uso –para poder facelo había uns requisitos específicos fixados e a norma establecía quen podía solicitar o informe de risco–, que datos debían usarse e con que finalidade –obxectivo específico–. A pesar de todo iso, o tribunal entende que non existen garantías axeitadas, dado que "non hai información suficiente para saber como operaba". Incide posteriormente a sentenza nesta cuestión ao criticar que o modelo de risco que se utiliza e os indicadores de risco sexan secretos e que iso impide que un suxeito interesado poida defenderse contra o feito de que se determinase un alto risco de fraude sobre el ou ela.

Nesta cuestión é onde, de aceptar esta lectura da sentenza, se viría prohibir ***de facto*** o uso deste tipo de ferramentas automatizadas para valorar riscos de incumprimento. En efecto, se se dá información suficiente para saber como opera a ferramenta –como parece exixir a sentenza comentada–, esta será inservible para os seus propios

[35] Isto foi posto de relevo pola doutrina en varias ocasións ao entender que esta tecnoloxía parece capaz de inferir certas características persoais baseadas noutros datos. É dicir, aínda que se prohiba solicitar datos en materia de afiliación sindical, relixión, sexo, orientación sexual ou discapacidade, os algoritmos son capaces de obter esta información a través doutros datos (CRAWFORD, K. e SCHULTZ, J., "Big data and due process: Towards a framework to redress predictive privacy harms", cit.). Por exemplo, a relixión ou a raza poden estar estatisticamente moi relacionadas co código postal ou o barrio onde vive a persoa. Así pois, tomar decisións baseadas na localización da vivenda resultará no fondo unha decisión baseada na raza ou, mesmo, conforme o tempo dedicado a ler unhas noticias en Facebook ou Google –e non outras– pódese predicir a afiliación política ou sindical. De feito, en moitos casos, descoñécense as capacidades dun algoritmo á hora de facer inferencias estatísticas, o que supón a "imposibilidade" de coñecer se o propio algoritmo está a tomar decisións fundamentadas en información discriminatoria ou non, en HARDT, M., "How big data is unfair", ***Medium***, 26 de septiembre de 2014. Dispoñible en: https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de.

[36] Malia ser certo que non se sabe se a Inspección finalmente decidía inspeccionar todos os suxeitos con risco alto –sen tomar ningunha decisión significativa– ou, pola contra, se esta intervención humana era relevante para a decisión final, unha cuestión que podería ser relevante para xustificar que a decisión final non era tomada polo algoritmo automaticamente.

obxectivos. Por unha banda, aqueles que tivesen un baixo risco e o soubesen[37] terían incentivos para incumprir coñecendo que as probabilidades de ser investigados son baixas. Por outra banda, os que tivesen un alto risco de ser inspeccionados e coñecesen "como opera o algoritmo" poderían modificar a súa conduta, non para cumprir, senón para enganar o sistema de valoración de risco –unha posibilidade que a doutrina puxo de manifesto en varias ocasións–[38]. En fin, na miña opinión, a transparencia no funcionamento do sistema de valoración de riscos de fraude non pode ser tal que lles permita aos suxeitos evadir a vixilancia e o control.

Tamén é certo que a sentenza apunta cara a outras posibilidades, dado que o tribunal sinala expresamente que bota en falta unha revisión previa por parte da Administración ou dun terceiro independente de que o algoritmo é proporcionado, vistos os dereitos en xogo e que, adicionalmente, non é discriminatorio. Esta posibilidade parece máis sensata. É dicir, dada a imposibilidade dunha transparencia absoluta para que o sistema sexa efectivo –o que ***de facto*** limita as posibilidades de defensa dos cidadáns–, tería sentido aceptar que a propia Administración ou un terceiro independente auditase o algoritmo para asegurar que funciona correctamente e sen nesgos.

Ademais, a sentenza parece esquecer que a decisión automatizada –de ser realmente automatizada, porque parece existir suficiente intervención humana cando o informe de riscos se envía á Inspección de Traballo– soamente ten como efecto que se inicie unha investigación –é un mero selector–, sendo a investigación a que determinará se hai sanción ou non. Con isto non quero dicir que a selección dos suxeitos a investigar non teña efectos sobre as persoas, pero, en calquera caso, as consecuencias non son absolutas nin irrevogables. A este respecto, soamente sinalo que a sentenza parece esquecer pór en proporción as garantías necesarias para poder tomar decisións baseadas nun algoritmo, cos efectos que a dita decisión produce[39]. É dicir, non sería proporcionado exixir as mesmas garantías para un algoritmo que adxudica risco de reincidencia dun delincuente cuxa consecuencia sexa ampliar o número de anos en prisión [Sentenza State ***v.*** Loomis, 881, N.W.2d 749, 7532 (Wis, 2016)] que as garantías necesarias para un algoritmo que dá apoio á Inspección para decidir que suxeito comezar a auditar, sendo a posterior análise e investigación realizadas completamente por persoas conforme o procedemento habitual.

En calquera caso, como se dixo, na miña opinión, esta sentenza ten outra lectura moi distinta á anterior. Débese partir de que esta sentenza responde a un tipo de ferramenta con finalidades moi concretas que pode ter levado a que o tribunal busque uns estándares de exixencia tan altos que ***de facto*** acabe prohibíndoa. As razóns son as seguintes: en primeiro lugar, afecta a persoas físicas. Ningún dos argumentos vistos nela parece aplicable a empresas, as cales non gozan do dereito á protección de datos

[37] Que non se informe os suxeitos de que teñen un baixo risco é un dos reproches "indirectos" que lle fai a sentenza á configuración do 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. e ZARSKY, T., "The algorithm game", cit., p. 46.

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

nin tampouco unha investigación pode ser considerada unha invasión da vida privada desta, xa que unha empresa non ten vida privada como dereito fundamental.

En segundo lugar, e esta podería ser a clave de bóveda da sentenza, a detección da fraude en materia de prestacións á Seguridade Social afecta a colectivos especialmente vulnerables que poderían merecer unha maior protección –maiores garantías– da súa vida privada. Como estableceron os demandantes, e o relator especial da ONU, este sistema "ten un efecto discriminatorio e estigmatizador", dado que se centra en investigar veciñanzas máis marxinadas e, con iso, "contribúe aos estereotipos e reforza unha imaxe negativa dos ocupantes das ditas veciñanzas". Falamos de persoas con incapacidades permanentes, invalidez ou en desemprego: cidadáns que, dunha forma ou outra, son especialmente vulnerables, polo que desenvolver unha ferramenta de máxima tecnoloxía para detectar fraude entre eles pode considerarse unha "criminalización da pobreza".

De feito, como sosteñen os expertos, a maior parte da fraude en Seguridade Social non provén polo cobramento de prestacións indebidas, senón pola falta de pagamento das cotizacións e pola economía informal[40]. Deste xeito, usar medidas invasivas da privacidade das persoas sen, pola súa vez, empregar as mesmas medidas para atacar as maiores fontes de fraude podería entenderse, en efecto, arbitrario, inxustificado ou, polo menos, desproporcionado.

Téñase en conta que, desde o momento en que dereitos fundamentais dos cidadáns entran en xogo –especialmente en colectivos socialmente vulnerables–, xa non debe actuar libremente o principio de discrecionalidade administrativa, senón que este virá limitado polos principios de necesidade e proporcionalidade. Desta forma, intentar xustificar esa medida invasiva dos dereitos fundamentais das persoas pola necesidade de evitar a fraude –necesidade lexítima en abstracto– cando non se está a atacar fontes de fraude maiores –economía informal, infracotización, etc.– e que, ademais, non requirirían da invasión de dereitos das persoas (dado que estes ilícitos son realizados por empresas) pode considerarse contrario a estes principios.

Por tales razóns, non creo que a doutrina desta sentenza deba entenderse como un impedimento xeral e abstracto ao uso do ***big data*** ou dos procesos automatizados para dar soporte ás decisións de selección de suxeitos infractores. Máis ben parece que a sentenza pode estar a oporse a unha política de "criminalización da pobreza" respecto a un goberno enfocando os seus esforzos –uso da máxima tecnoloxía dispoñible– para detectar a pequena fraude de persoas en xeral en situacións vulnerables, á vez que pouco se fai na mesma liña pola loita contra a gran fraude (violando os principios de necesidade e proporcionalidade con iso).

En fin, poucas dúbidas caben da necesidade de garantir os dereitos fundamentais das persoas fronte ao Estado e, en especial, evitar nesgos discriminatorios. Ao mesmo tempo, pouco sentido tería limitar as posibilidades de adaptación das administracións ao século XXI permitindo usar os seus recursos máis eficientemente, á vez que conseguen recompensar mellor os suxeitos cumpridores a través dunha menor

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

probabilidade de ser obxecto dunha inspección. Desta forma, a lei debe preocuparse especialmente de que o sistema funcione –que as razóns de elección non respondan a nesgos ou discriminacións, senón a unha verdadeira maior probabilidade de infrinxir a norma– e que exista suficiente transparencia para que o sistema poida ser axuizado en caso de presentar indicios de arbitrariedade ou de discriminación.

5 Síntese dos retos legais na implantación do *big data* como método de selección de suxeitos a investigar e algunhas recomendacións

A pesar de que a selección dun ou outro suxeito, para iniciar unha inspección, está configurada xuridicamente como unha decisión discrecional da Administración, o uso de ferramentas automatizadas para a construción de perfís de risco de incumprimento da normativa presenta múltiples conflitos xurídicos, especialmente en materia de protección de datos, protección da intimidade e posibles discriminacións. Desta forma, a Administración, no deseño da ferramenta informática, deberá ter en conta estes dereitos e establecer garantías que protexan os dereitos fundamentais dos cidadáns.

A intensidade desas garantías é unha cuestión actualmente moi debatida pola doutrina e os tribunais, sen que exista consenso. Non obstante, si se poden fixar unha serie de pautas a seguir.

En primeiro lugar, deberase valorar a necesidade do uso da ferramenta, entendida como a existencia dun obxectivo lexítimo –neste caso a loita contra a fraude–. Non obstante, non parece suficiente unha xustificación abstracta da necesidade de alcanzar ese obxectivo, senón concretamente da relación entre a consecución dese obxectivo e o uso da ferramenta automatizada (adecuación). Deste xeito, como se viu neste traballo, podería entenderse que, se se quere perseguir a fraude –finalidade lexítima en abstracto–, non debería utilizarse unha ferramenta automática de selección de perfís contra pequenos defraudadores se non se usa para grandes defraudadores –que sería a forma de alcanzar verdadeiramente o obxectivo–.

En segundo lugar, a proporcionalidade. En efecto, as garantías para salvagardar os dereitos dos cidadáns deben ser proporcionadas respecto ao dano que a ferramenta informática pode xerar. Desta forma, non será o mesmo unha ferramenta que estableza perfís de risco de reincidencia cuxo uso pode implicar a prolongación dunha pena privativa de liberdade que as garantías que debe ter un sistema que establece un risco de cometer unha infracción laboral cuxa única posible consecuencia é o inicio dunha investigación, a cal será a que determine, en última instancia, se existiu ou non ilícito.

En terceiro lugar, non será o mesmo unha ferramenta informática que se limite a procesar datos que xa constan en poder da Administración pública que outra que se dedique a escanear Internet co obxecto de reunir datos para a vixilancia e control da normativa. En efecto, as posibilidades tecnolóxicas son múltiples e non todas teñen a mesma repercusión. Desta forma, deberanse exixir maiores garantías a unha ferramenta que recompila datos sen consentimento dos interesados que a outra que

soamente os procesa co fin de axudar a tomar decisións acertadas respecto á selección de suxeitos que se van investigar.

En cuarto lugar, a cuestión máis complexa de resolver será a necesidade de transparencia. Poucas dúbidas caben de que, para garantir o dereito de defensa do afectado e para evitar discriminacións directas ou indirectas, é imprescindible que o proceso de selección sexa transparente. Non obstante, a pesar de que isto sexa así, cando o algoritmo ten por obxectivo, concretamente, a loita contra a fraude, a transparencia –máis ben o exceso dela– pode deixar inoperativa a propia ferramenta.

En efecto, a información respecto a como funciona o algoritmo pode desvelar información clave que, por unha banda, incremente o incumprimento e, por outra, lle permita a un incumpridor reducir o risco de ser detectado. Por esta razón, aínda que se comparta a necesidade da "transparencia algorítmica", parece recomendable buscar outras fórmulas que non frustren os resultados desexados. Neste traballo expóñense dúas: i) publicar que datos se subministran á ferramenta para tomar as súas decisións, xa que isto eliminaría as posibilidades de que se utilicen datos sensibles ou discriminatorios: ii) outra posibilidade podería ser que, internamente ou a través dun organismo especializado independente, se realizase unha análise de verificabilidade da ferramenta informática que comprobase que non se usan datos prohibidos e que os resultados non son discriminatorios.

Por último, débese sinalar que a protección, as garantías e as salvagardas fronte á ferramenta non teñen por que ser as mesmas se o informe sobre probabilidade de incumprir a normativa se fai respecto dunha empresa que se se fai sobre unha persoa física. Por iso, parece recomendable para a Administración establecer dous sistemas diferenciados de selección, para que, deste xeito, ademais de poder fixar estándares de garantía distintos en caso de que se queira, no suposto de que se impugnase o sistema –e ante unha eventual anulación ou prohibición de uso deste–, o tribunal puidese valorar por separado a licitude de cada un.

6 Conclusións: vantaxes e límites do uso do *big data* na inspección

6.1 Beneficios achegados

O uso das ferramentas do ***big data*** e a intelixencia artificial permite a planificación estratéxica e a selección de suxeitos a inspeccionar para mellorar o uso dos recursos da Inspección[41]. Estes mecanismos son capaces de clasificar cada empresa baseada no seu risco de incumprimento[42]. Desta forma, extraendo información e patróns ocultos, mellórase a ratio de acerto, atopando máis incumprimentos, á vez que se reducen

[41] WATKINS, R.C., REYNOLDS, K.M., DEMARA, R., GEORGIOPOULOS, M., GONZÁLEZ, A. e 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.

as inspeccións en empresas que cumpren. En particular, o ***big data*** proporciona as seguintes vantaxes ao sistema:

1. Redúcese o tempo e os recursos dedicados á análise manual de datos.

2. Permítese unha rápida curva de aprendizaxe dos novos inspectores sen que sexan necesarios anos de experiencia para desenvolver intuicións sobre onde buscar os incumprimentos.

3. Localízanse patróns e tendencias de incumprimento indetectables pola intuición a través da correlación de datos.

4. Permite a planificación de campañas de forma máis eficiente.

5. Proporciona a posibilidade de detectar e atallar as chamadas "epidemias" de fraude antes de que se expandan.

6. A selección baseada en datos incrementa unha visión mediopracista ou longopracista dos obxectivos. Isto reduce as posibilidades de tomar decisións "a golpe de telexornal". Isto é, decisións baseadas en sucesos puntuais que modifican o curso da acción inspectora pola relevancia momentánea dun feito e non porque existan verdadeiras razóns xustificativas de tal actuación[43].

7. As técnicas do ***big data*** tamén melloran a avaliación da actuación inspectora en termos xerais. Dun lado, permite definir o nivel de incumprimento nun país ou sector e como este diminúe grazas ás actuacións da Administración. Iso incrementará a lexitimidade social da necesidade da Inspección, baseándose en datos nun mundo en que aquilo que non pode medirse poucas veces se ten en conta.

8. Estas técnicas de tratamento de datos tamén facilitan a súa propia avaliación para mellorar cada día a través do ***feedback*** dos inspectores.

En fin, cada vez máis países adoptan estas técnicas para mellorar a selección de suxeitos a inspeccionar con notable éxito. Austria, tras a inclusión destas técnicas baseadas en riscos de incumprimento para a selección, pasou de atopar entre 20 e 30 fraudes por cada 100 inspeccións realizadas a descubrir incumprimentos de entre o 60 e o 80% das inspeccións efectuadas[44]. Adicionalmente, este sistema permitiu tamén incrementar o cumprimento voluntario a través das comunicacións (cartas), avisando da información que se tiña. A selección previa permitiu que o cumprimento pasase de producirse nun 7% dos que recibían a carta a un 20 ou 30%[45].

6.2 Límites no uso do ***big data***

Malia as oportunidades que brinda a aplicación destas modernas técnicas para mellorar a efectividade das inspeccións, a súa incorporación exixe ter os datos con calidade suficiente e unha aposta segura por estes. Todo iso non sempre é posible ou sinxelo.

1. En primeiro lugar, o ***big data*** necesita nutrirse de suficientes datos de calidade para poder obter conclusións válidas. Isto implica xuntar todos os datos nunha mesma ferramenta informática coa colaboración doutras administracións (CC. AA.) e outras ramas da Administración estatal (Facenda, DXT, etc.). Neste sentido, no noso país

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

[44] Nos dous casos, o índice de acerto na selección era mellor que seleccionar de xeito aleatorio, cuxo índice era do 15-20%.

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

fixéronse moitos avances, pero débese recordar que cantos máis datos se teñan maior fiabilidade existirá[46].

2. Adicionalmente a ter os datos, estes non deben estar nesgados ou incompletos. Por exemplo, se no pasado se focalizou nun determinado tipo de empresas –onde loxicamente se terán atopado incumprimentos– e eses son os datos que se subministran á ferramenta, baseándose neses datos considerarase que estas empresas son as que deben ser inspeccionadas no futuro. Isto, pola súa vez, implicará maior número de fraudes atopadas nesas empresas, confirmando o nesgo e pechando o círculo[47]. Por esta razón, é tan importante que os datos subministrados sexan completos, de calidade e sen nesgos manifestos.

3. Tamén será necesario darlles formación aos inspectores sobre a utilidade da ferramenta e como usala, ademais de proporcionarlles formación para que sexan capaces de dar ***feedback*** a esta[48].

4. Outra cuestión que pode limitar o uso da ferramenta é a desconfianza ao novo. Toda organización adoita sentirse máis cómoda facendo as cousas como as sabe facer, e a inclusión de novos mecanismos provoca rexeitamento. Por esta razón, é importante que se coñeza o funcionamento e as mecánicas subxacentes á ferramenta, de tal forma que se xere confianza no seu uso[49].

5. Débese sinalar que o ***big data*** non obxectiviza o uso dos recursos, soamente fai máis eficiente esa utilización. Por esta razón, seguirá sendo necesaria a incorporación dos coñecementos e experiencias dos inspectores, así como a reflexión e a toma de decisións sobre priorización. O sistema de ***big data*** en ningún caso substitúe a necesidade dunha planificación estratéxica nin elimina o uso da discrecionalidade administrativa para elixir obxectivos. O ***big data*** é unha ferramenta que axuda a esa toma de decisións e a elixir eses obxectivos.

6. Por último, estas ferramentas poden acabar sendo usadas para xustificar a persecución de certos colectivos historicamente discriminados. Sobre todo en materia de policía, criticouse que se usen estas ferramentas para xustificar unha maior vixilancia nos barrios pobres ou a detención en aeroportos de persoas de cor[50]. En efecto, neste traballo púxose de manifesto o perigo de que os mecanismos se utilicen para xustificar un uso dos recursos enfocados en investigar máis pequenas empresas ou receptores de prestacións. Por iso, estes sistemas de selección requiren unha constante vixilancia e crítica como calquera outro dos existentes.

---

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. Dispoñible en: https://kth.diva-portal.org/smash/get/diva2:1238767/FULLTEXT01.pdf (Consultado o 6 de abril de 2020).

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

49 WATKINS, R.C., REYNOLDS, K.M., DEMARA, R., GEORGIOPOULOS, M., GONZÁLEZ, A. e 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. e 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.

Neste sentido, será necesario establecer controis internos e externos para asegurar que os dereitos fundamentais das persoas non son violados. Dun lado, a Administración ten a obriga de que a selección non responda a patróns discriminatorios –nin voluntarios (subministrando datos protexidos) nin involuntarios (subministrando datos que por erro están nesgados)–. Doutro lado, cómpre que a selección e o uso da ferramenta sexan transparentes. Por suposto, isto non pode implicar a obriga para a Administración de publicar o resultado da análise de risco –baixo a ameaza de que iso se utilice para infrinxir a norma–, senón que se debe publicar que datos son tidos en conta, de forma xeral, polo ***big data*** para crear o índice de risco.

Bibliografía

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

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

BAMBUER, J. e 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)", ***World Compliance Association***, 2020. Dispoñible 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. e 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. Dispoñible en: https://dl.acm.org/doi/10.1145/312129.312224 (Consultado o 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,*** Bruxelas, 2006. Dispoñible 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, Bruxelas, 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. e 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 febreiro de 2020. Dispoñible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAyNDa3NDJUK0-stKs7Mz7M1MjACC6rl5aekhrg425bmpaSmZealpoCUZKZVuuQnh1QWpNqmJeYUp6qlJuXnZ6OYFA8zAQCfSdkrYwAAAA==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. Dispoñible 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 o 3 de outubro de 2017).

GUPTA, M. e 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 setembro de 2014. Dispoñible 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.

OECD, ***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. Dispoñible en: https://kth.diva-portal.org/smash/get/diva2:1238767/FULLTEXT01.pdf (Consultado o 6 de abril de 2020).

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

SANDERS, C.B. e 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. Dispoñible en: http://upit.es/web/index/show/id/36 (Consultado o 6 de abril de 2020).

WATKINS, R.C., REYNOLDS, K.M., DEMARA, R., GEORGIOPOULOS, M., GONZÁLEZ, A. e 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.