Colección

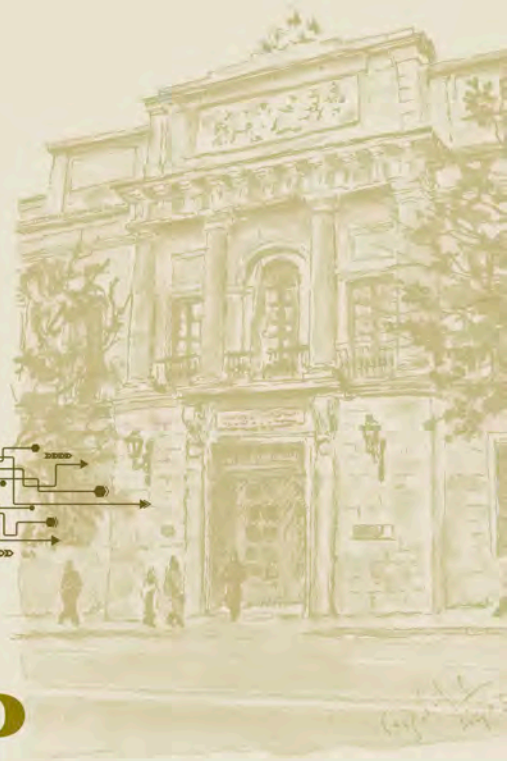
INNOVACIÓN PÚBLICA

Repensando la Administración pública

Administración digital e innovación pública

Coordinador

Carles Ramió



INAP

INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA

REPENSANDO LA ADMINISTRACIÓN PÚBLICA

ADMINISTRACIÓN DIGITAL E INNOVACIÓN PÚBLICA

Carles Ramió
(coordinador)

Carles Ramió
J. Ignacio Criado
Concepción Campos Acuña
Miquel Salvador
Lorenzo Cotino Hueso
Andrés Pastor Bermúdez
Lucía Escapa Castro
Luis F. Aguilar
Amalio Rey
María Dapena Gómez
Mikel Gorriti Bontigui
Michael Donaldson Carbón
Guillem Ramírez Chico
Fermín Cerezo Peco
Àngel Cortadelles i Bacaria

INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA
MADRID, 2021

Colección: INNOVACIÓN PÚBLICA

FICHA CATALOGRÁFICA DEL
CENTRO DE PUBLICACIONES DEL INAP

REPENSANDO la Administración pública. Administración digital e innovación pública / coordinador, Carles Ramió ; [autores, J. Ignacio Criado… et al.]. – 1ª ed. – Madrid : Instituto Nacional de Administración Pública, 2021. – 439 p. ; 24 cm. – (Colección INNOVACIÓN PÚBLICA)

Bibliografía

ISBN 978-84-7351-711-9 (formato papel). – ISBN 978-84-7351-712-6 (formato electrónico). – NIPO 278-21-001-6 (formato papel). – NIPO 278-21-002-1 (formato electrónico)

1. Internet en la administración pública-España. 2. Administración pública-Innovaciones tecnológicas-España. I. Ramió, Carles, coord. II. Criado, J. Ignacio. III. Instituto Nacional de Administración Pública (España). IV. Serie

35(460): 004.738.5

Primera edición: enero 2021

Catálogo general de publicaciones oficiales:
http://publicacionesoficiales.boe.es

La actividad editorial del Instituto Nacional de Administración pública está reconocida por Scholary Publishers Indicators in Humanities and Social Sciences (SPI) en las disciplinas de Ciencias Políticas y Derecho. El listado SPI es aceptado como listado de referencia por la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA), por la Comisión Nacional Evaluadora de la Actividad Investigadora CNEAI y por la ANEP (Agencia Nacional de Evaluación y Prospectiva).

Edita:
INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA
www.inap.es

ISBN: 978-84-7351-711-9 (formato papel). – ISBN: 978-84-7351-712-6 (formato electrónico)
NIPO: 278-21-001-6 (formato papel). – NIPO: 278-21-002-1 (formato electrónico)
Depósito Legal: M-1730-2021

Preimpresión: Dagaz Gráfica, s.l.u.
Impresión: SAFEKAT

En esta publicación se ha utilizado papel reciclado libre de cloro de acuerdo con los criterios medioambientales de la contratación pública.

ÍNDICE

CAPÍTULO 5

HACIA LA TRANSPARENCIA 4.0: EL USO DE LA INTELIGENCIA ARTIFICIAL Y *BIG DATA* PARA LA LUCHA CONTRA EL FRAUDE Y LA CORRUPCIÓN Y LAS (MUCHAS) EXIGENCIAS CONSTITUCIONALES

Lorenzo Cotino Hueso[1]
Catedrático de Derecho Constitucional
Universitat de Valencia

1. DE LA TRANSPARENCIA 1.0 A LA 4.0. PONIENDO A LAS «MÁQUINAS» A RASTREAR TODOS LOS DATOS DE LA ADMINISTRACIÓN, Y MÁS ALLÁ

El juez del Tribunal Supremo americano Luis B. Brandeis afirmó que «la luz del sol es el mejor desinfectante»[2] (Brandeis, 1913). Por lo que ahora interesa, la transparencia pública es un instrumento de garantía de la eficacia, eficiencia, objetividad, legalidad, de buena administración (Arena, 1993: 14 y ss.). Y no solo se trata de un control por posibles responsabilidades penales y estrictamente jurídicas, sino las responsabilidades políticas y la dación de cuentas (Ballart y Ramió, 2000: 527). Arena (1993: 13) afirmaría que «el

[1] El presente estudio es resultado de proyecto «Derecho y big data», Grupo de Investigación en Derecho Público y TIC, Universidad Católica de Colombia; proyecto «La regulación de la transformación digital y la economía colaborativa», PROMETEO/2017/064 y MICINN Retos, «Derechos y garantías frente a las decisiones automatizadas…» (RTI2018-097172-B-C21, pendiente), estancia de investigación ayuda Generalitat (AEST/2019/013).

[2] «Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman».

pueblo soberano que mira dentro del palacio no se limita a levantar acta, sino que juzga lo que ve».

La transparencia ha dado un salto desde Brandeis a Obama (Cotino, 2013). Así, la transparencia exige que la información no espere a ser solicitada por el ciudadano ejerciendo su derecho de acceso a la información, sino que la información vaya proactivamente al ciudadano, de la mano de internet. Así, especialmente se ha ido conformando la obligación de que unos ítems de información mínima que deben brindarse por las Administraciones en sus portales de transparencia. De este modo, se imponen importantes obligaciones jurídicas de «transparencia activa», es decir, de mínimos de información obligatorios de relevancia jurídica, política, social o económica que deben ser satisfechos en portales de transparencia. Todo ello se fundamenta en la máxima penitenciaria de Bentham «cuanto más estrictamente nos vigilan, mejor nos comportamos» bajo el modelo del panóptico, sobre esta base y bajo el principio de que la luz es el mejor desinfectante, la transparencia desincentiva malas conductas en la sociedad y la corrupción.

Gracias a internet, hemos creado un panóptico en dos direcciones, de un lado, que ahora no interesa, los individuos nos hemos hecho totalmente transparentes y, por tanto controlables. Pero, por lo que ahora interesa y del reverso, cada ciudadano es un potencial centinela que está en una torre de vigilancia el centro de todos los poderes públicos, a los que puede observar a golpe de *clic*. En la línea de ser el mejor desinfectante, el efecto fundamental de la transparencia es su potencialidad misma. Su virtud va más allá del ejercicio real de control por la ciudadanía y sectores interesados y de los particulares accesos a información que se ejerzan y el uso que hagan de los portales de publicidad activa con la cada vez más nutrida información. Sin embargo, en buena medida los ciudadanos no van a perder el tiempo ejerciendo este derecho (Dyrberg, 1999: 158), o al llegar a casa por la noche preferirán ver una serie o un partido de fútbol antes de entrar en el portal de contratación de su municipio. El *centinela* muy posiblemente está *dormido en la garita* y debemos consolarnos en que los controlados no sepan que no se les está controlando. Debemos confiar en que la fuerza de la transparencia reside en su papel de agente de cambio cultural de las organizaciones públicas que saben que pueden ser observadas. Y es que con transparencia desde el último empleado público hasta el primer responsable son conocedores de que todas sus actuaciones —u omisiones— son susceptibles de ser revisadas por la ciudadanía, no solo por los interesados directos, sino por todos y cada uno de los miembros de la sociedad en la que actúan (Curtin, 2000: 8). Sin embargo, es posible dudar de dicho efecto inhibidor por falta de atención por la ciudadanía. Puede cuestionarse hoy día que haya un vínculo significativo entre la transparencia, su incremento con las TIC y la reducción de la corrup-

ción (Galetta, 2017: 13). Se difunden a un clic ingentes cantidades de información, de magnitudes casi cósmicas. Se corre también el peligro de que dicha información casi ilimitada puede generar más oscurantismo y opacidad por lo que se ha llamado, *infoxicación*, esto es, exceso o sobrecarga de información.

En este proceso de difusión activa de información pública, se trata, además, de ir poniendo la información de modo reutilizable, esencialmente, que se difundan datos e información legibles por máquinas. Ello es esencial en el ámbito de la reutilización desde la Directiva 2013/37/UE y especialmente en la Directiva (UE) 2019/1024 de 20 de junio de 2019 (Considerando 35, art. 2.13.º[3], arts. 5.1.º y 8.º, 9.1.º, 14.1b). Sin embargo no es una exigencia jurídica clara, sino un principio preferente a fomentar en el ámbito de la transparencia y la publicidad activa (arts. 5.1.º y 11, Ley 19/2013).

Que la información sea procesable automatizadamente facilita, si se me permite, que pueda cerrarse más el círculo. Ya no se tratará de que se pueda controlar el ejercicio del poder público, sino que efectivamente se controle en razón de la última revolución tecnológica… merced a sistemas inteligentes, automatizados y algoritmos. Ya que nosotros no parecemos muy interesados en ejercer nuestros derechos y posibilidades de controlar el ejercicio del poder público, ya que el centinela está dormido y los vigilados lo saben, pongamos a las *máquinas* a trabajar. De hecho, algunas leyes que obligan a poner a disposición ingentes cantidades de datos de cuentas abiertas (como la valenciana, de Extremadura, Aragón o La Rioja) ciertamente no son más que un ejercicio vacuo de exhibicionismo si no van acompañadas de sistemas automatizados para analizar dichos datos.

Pero la transparencia y la lucha contra la ilegalidad pretende ir mucho más allá. Bajo el nuevo paradigma de la transparencia y la apertura por defecto y en el marco de la transformación digital, se impulsa que los sistemas automatizados incluyan entre los datos e información a analizar no solo la creciente información pública de los portales, sino, también, se trata de poner a trabajar a las máquinas sobre todos los datos para la actuación material y procedimental y prestación de servicios públicos que tienen las Administraciones Públicas. Es más, incluso, respecto de los datos y la información que la ciudadanía hace pública en plataformas y redes. Aunque todo esto se pueda hacer técnicamente, lo cierto es que los presupuestos de requerimientos jurídicos y límites no son pocos.

---

[3] «13) "Formato legible por máquina": formato de archivo estructurado que permita a las aplicaciones informáticas identificar, reconocer y extraer con facilidad datos específicos, incluidas las declaraciones fácticas y su estructura interna».

2. SISTEMAS AUTOMATIZADOS E INTELIGENCIA ARTIFICIAL CONTRA EL FRAUDE. HOLANDA, FRANCIA Y LO POCO QUE SABEMOS EN ESPAÑA

Desde 2006 la Comisión Europea (2006: 10, 25 y, en especial 83 y ss.) (o Watkins *et al*. desde 2003) postulan el uso de herramientas automatizadas para la planificación estratégica de las administraciones de control, para localizar los focos de mayor riesgo para centrar los objetivos de inspección. Más recientemente se afirma desde la OCDE (2018: 38-40, Criterio n.º 8) que «las tecnologías de la información y la comunicación deben utilizarse para maximizar la concentración en el riesgo, la coordinación y el intercambio de información, así como el uso óptimo de los recursos». Ahora bien, precisamente las cuestiones clave que se definen al respecto son precisamente la necesidad de una legislación de calidad que defina atribuciones, órganos, procedimientos y derechos claramente, así como recursos a este tipo de decisiones y una fuerte transparencia y proporcionalidad frente a la discrecionalidad.

Desde la UE en julio de 2020 se han definido cinco usos de IA públicos (Misuraca y Van Noordt, 2020, siguiendo a Engstrom *et al*., 2020). En nuestro caso nos encontraríamos en el uso de la IA para la aplicación de la ley, que incluiría identificar o priorizar los objetivos que requieren aplicación o inspecciones. Y entre las 10 tipologías de IA en los servicios públicos (Misuraca y Van Noordt, 2020: 2.1.1, siguiendo a Wirtz *et al*., 2019), la más afín es la de análisis predictivo, simulación y visualización de datos. Estas soluciones de IA aprenden de los grandes conjuntos de datos para identificar patrones en los datos. No obstante, serían cercanas algunas tipologías como los sistemas expertos y basados en reglas, toma de decisiones algorítmicas, los mismos que se diseñan para facilitar o automatizar plenamente los procesos de toma de decisiones de posible relevancia. También pueden darse o quedar integrados tipos de IA como la gestión del conocimiento u otros tipos más alejados como el reconocimiento de audio, de vídeo y de procesamiento de lenguaje natural, minería de textos y análisis del habla que bien puede servir para pasar a formatos y soportes procesables o el tipo de IA de reconocimiento de identidad.

Recientemente Todolí (2020: 315, 332) recuerda que las herramientas automatizadas o inteligentes pueden reducir el tiempo y los recursos a emplear, ayudar a los inspectores humanos a su aprendizaje a partir de nuevos patrones y tendencias de incumplimiento que serían indetectables por la experiencia e intuición humanas. Sirven a la planificación eficiente a medio y largo plazo y no a golpe de noticias o escándalos, detectar y atajar a tiempo nuevas modalidades y prácticas de fraude, permite evaluar mejor la actividad y control realizadas y todo ello legitima la propia actividad de control e inspección (Watkins: 12). Es más, esta eficacia se percibe por los potenciales

inspeccionados y lleva a un mayor cumplimiento normativo. Obviamente ello tiene toda una serie de requerimientos y controles, así como formación y la continuidad del conocimiento y actividad humanos. Y señala Todolí que las actividades de inspección de hacienda, impuestos, seguridad social, laboral, antifraude y corrupción, etc. por lo general no tienen una tasa de éxito muy alta. Es decir, se generan muchas molestias al sector inspeccionado que sí que cumple la norma, algo que se puede evitar afinando mejor los objetivos.

Se siguen ahora más de cerca tres sistemas automatizados para el control del fraude por cuanto son referencia en tanto en cuanto que han sido analizados constitucionalmente muy recientemente por los más altos tribunales. Así el sistema holandés declarado contrario a derechos fundamentales y la ley de finanzas francesa que sí que ha admitido la constitucionalidad de la regulación. El sistema valenciano ha sido muy negativamente valorado por la AEPD (2017) y cabe adelantar que no alcanzaría los estándares de los otros sistemas para su admisión constitucional.

2.1. **El sistema holandés de tratamiento automatizado, profundo y predictivo de datos ilimitados SyRI, declarado contrario a los derechos fundamentales**

He tenido ocasión de analizar con detalle (Cotino, 2020). La amplia y fundamentada sentencia de 5 de febrero de 2020 del Tribunal de Distrito de la Haya (C/09/550982/HA ZA 18-388) declara contrario al artículo 8 CEDH sistema *Systeem Risicoindicatie* (SyRI), en concreto su regulación por la sección 65 de la Ley SUWI y el capítulo 5.º del Decreto SUWI. El texto es accesible en inglés (y neerlandés)[4]. El sistema SyRI es un instrumento legal y tecnológico para detectar diversas formas de fraude, incluidos beneficios sociales, subsidios y fraude fiscal. Para ello genera informes de riesgo, esto es, determina «que una persona jurídica o física se considera digna de ser investigada con respecto a un posible fraude, uso ilegal e incumplimiento de la legislación» (3.2, Ley SUWI secc. 65. 2.º y 4.12).

El sistema SyRI «implica un procesamiento de datos estructurado basado en archivos existentes y disponibles» (6.61). Uno de los elementos decisivos para considerar que el sistema vulnera derechos fundamentales es que se manejaba una —casi ilimitada— «cantidad de datos sustancial» (6.50): 17 categorías detalladas (art. 5a.1. 3.º, Decreto SUWI) sobre trabajo, sanciones administrativas, datos fiscales, bienes muebles e inmuebles, beneficios sociales, datos comerciales, de vivienda, de identificación, de integración

[4] <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878>.

cívica, cumplimiento de la legislación, educación, pensiones, deudas, permisos y exenciones, si está asegurada por la Ley de Seguro de Salud (4.17). El tribunal llega a afirmar que «es difícil imaginar cualquier tipo de datos personales que no sean elegibles para el procesamiento en SyRI» (6.98).

Frente a lo que sostiene el Estado (6.45), el tribunal argumenta que la ley regula un sistema que puede llegar a ser de «autoaprendizaje y aprendizaje profundo» y de análisis predictivo de riesgos, aunque «no hay información suficiente para saber cómo operaba» (6.49) y «no se hace uso en este momento» de tales utilidades (6.51). También afirma que el tratamiento que realizaba queda bajo el ámbito del artículo 22 RGPD: el perfilado de riesgos «una decisión con efecto legal, o al menos una decisión que afecta significativamente a los interesados» (6.57). Además, se considera que no hay «intervención humana significativa», pues no es suficiente la eliminación de falsos positivos que se da (6.57). Pese a que se dedican prolijas argumentaciones, lo cierto es que no se da una clara conclusión del hecho de que se trate de un sistema de aprendizaje profundo o bajo el régimen del artículo 22 RGPD. Cabe considerar que estas argumentaciones lo que pretenden es subrayar más si cabe la importancia de las garantías compensatorias que se requieren para efectuar tratamientos de datos.

Sin perjuicio de los detalles, la sentencia que analiza y considera contrario a derechos fundamentales este sistema, aplica un canon de control más estricto por el deber de «responsabilidad especial cuando aplican nuevas tecnologías» de los Estados (6.6 y 6.84) y en concreto el legislador de SyRI (6.85). Aunque el sistema estaba regulado legal y reglamentariamente de modo muy preciso, se entiende que la «legislación no alcanza el "equilibrio justo" requerido por el CEDH» (6.7): hay «salvaguardas insuficientes debido a la gran cantidad de datos, de varios tipos y de una gran cantidad de fuentes diferentes, que pueden procesarse. Además, no se conocen los indicadores de riesgo y el modelo de riesgo ni los criterios objetivos que subyacen a la validez de los indicadores de riesgo y el modelo de riesgo» (6.102).

2.2. **La automatización de grandes datos por la ley francesa para 2020, declarada constitucional**

Resulta de interés la Decisión 2019-796 DC de 27 de diciembre del Consejo Constitucional francés, de 147 apartados, sobre la Loi de finances para 2020[5].

[5] Acceso en: <https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2019-796-dc-du-27-decembre-2019-communique-de-presse#:~:text=Par%20sa%20d%C3%A9cision%20n%C2%B0,dernier%2C%20de%20plus%20de%20soixante>.

La ley permite por un período de tres años, a las administraciones tributaria y aduanera «utilizar medios informáticos y automatizados para recopilar y utilizar el contenido accesible en los sitios web de los operadores de plataformas que conectan a varias partes con miras a la venta de un bien, el suministro, un servicio o el intercambio o compartir contenido, bienes o servicios. Así pues, le permiten, por un lado, recopilar de manera indiferenciada grandes volúmenes de datos, relacionados con un gran número de personas, publicados en dichos sitios y, por otro lado, utilizar estos datos, utilizándolos, agregando y haciendo verificaciones cruzadas y correlaciones entre ellos» (n.º 83). De este modo se pretende «reforzar los medios de control de las administraciones tributaria y aduanera, dotándolas de sistemas informatizados y automatizados de exploración de los datos personales hechos públicos en internet, a efectos de investigación y persecución de infracciones en materia tributaria y aduanera» (n.º 84). Como luego se expone, el Consejo Constitucional admite el sistema por considerar que el legislador ha regulado proporcionalmente suficientes garantías frente a los riesgos para la privacidad y otros derechos.

2.3. **Los opacos sistemas automatizados o inteligentes antifraude en España y el sistema SALER (o SATAN) valenciano**

Desde la Red de Derecho Administrativo de la IA (Red DAIA) hemos criticado y mucho que no haya un mapeo de los usos de IA en el sector público, algo que afortunadamente desde Cataluña se está empezando a evitar, señalando 50 casos de uso (ACPD, 2020). De hecho, considero que sería una obligación legal difundir estos tratamientos en razón del artículo 6 bis de la Ley 19/2013, de 9 de diciembre, de transparencia, respecto del inventario de actividades de tratamiento en aplicación del artículo 31 de la Ley Orgánica 8/2018. Es muy posible que administraciones punteras como tributarias, de seguridad social, la Comisión Nacional del Mercado y la Competencia y otras estén usando sistemas automatizados y avanzados para la detección y lucha contra el fraude. Sin embargo y lamentablemente, ni lo sabemos y solo muy recientemente Gutiérrez (2020) en diciembre ha elaborado un listado de contratación pública de este tipo de sistemas. Asimismo, en octubre de 2020 la Tesorería General de la Seguridad Social anuncia la contratación de servicios de Accenture para detectar falsos autónomos y empresas ficticias. Siendo los pliegos de condiciones de todo interés[6].

[6] Pliego de condiciones en: <https://www.ecestaticos.com/file/63657ccbb42dcd76e15ce5ecf2397e41/1603306235-pliego-de-condiciones-te-cnicas.pdf>.

El Plan Estratégico de la Agencia Tributaria 2020-2023 afirma que «la utilización de las nuevas herramientas informáticas que permite configurar un sistema completo y dinámico de riesgos para, progresivamente, ir detectando de forma más automatizada y extensa actuaciones y conductas de riesgo de deudores que, hasta ahora, solamente afloraban y se combatían al analizar individualmente cada caso». Se afirman en esta línea actuaciones de gestión recaudatoria y, en particular, «programas de investigación recaudatoria», en base a la detección de tramas y actividades fraudulentas (Agencia Tributaria, 2020; 108, A. 4).

Sin embargo, la cuestión se pierde una gran opacidad y la huida del Derecho está servida. Posiblemente sea el secreto mejor guardado con la ayuda del actual ordenamiento jurídico. Los planes de control tributario son «reservados», sin perjuicio de «que se hagan públicos los criterios generales que lo informen» (artículo 116, Ley 58/2003, de 17 de diciembre, General Tributaria). Y el carácter reservado se extiende a los medios informáticos y sistemas de selección. Así, el artículo 170.7 del Real Decreto 1065/2007, de 27 de julio (Reglamento General de actuaciones y procedimientos de gestión e inspección tributaria) dispone que «los planes de inspección, los medios informáticos de tratamiento de información y los demás sistemas de selección de los obligados tributarios que vayan a ser objeto de actuaciones inspectoras tendrán carácter reservado, no serán objeto de publicidad o de comunicación ni se pondrán de manifiesto a los obligados tributarios ni a órganos ajenos a la aplicación de los tributos». Asimismo, se trata de una fase de la actuación administrativa en buena medida inmune al control judicial. No en vano, la determinación de los obligados tributarios que vayan a ser objeto de comprobación «tiene el carácter de acto de mero trámite y no será susceptible de recurso o reclamación económico-administrativa» (art. 170.8.º Real Decreto 1065/2007). Es más, la Administración tributaria ni siquiera queda vinculada por sus propios planes de inspección. Como recuerda recientemente el TS, no hay un «derecho subjetivo del contribuyente a no ser investigado si no se encuentra incluido en dichos planes y programas, pues ello supondría el incumplimiento por parte de la Administración del deber de fiscalización de que todos los ciudadanos cumplan con el deber de contribuir» (sentencia 236/2020, de 19 de febrero, recurso de casación 240/2018).

En consecuencia, la parte más sustancial escapa a nuestro conocimiento y, de momento, hay que ceñirse al único sistema cuya existencia se conoce, que es el sistema de alertas tempranas (SALER, inicialmente llamado SATAN) configurado por los artículos 17-36 de la Ley 22/2018, de 6 de noviembre, de la Generalitat de la Comunidad Valenciana. Al parecer, el sistema anunciado desde 2017 ha sido desarrollado, entre otros, por el conocido y refugiado en España Falciani. Y bien es cierto que más allá de la propia ley, no es

sencillo saber sobre la naturaleza y funcionamiento de dicho sistema. Es por ello que quien suscribe el 29 de julio de 2020 ejerció un derecho de acceso a la información pública[7] y las respuestas logradas son posiblemente la única información al respecto. Cerrado este trabajo se ha conocido un estudio sobre el sistema (Criado, Valero y Villodre 2020).

Según el artículo 17.1.º, «el sistema de alertas se articulará a través de un conjunto de herramientas cuya interacción permite la detección de posibles irregularidades y malas prácticas administrativas, con carácter preventivo, a partir del análisis de la información obtenida y de la evaluación de factores de riesgo que potencialmente pudieran originarlas». El sistema se integra por datos y bases de datos de diversa procedencia, un «sistema lógico e informático de procesamiento de datos» y la evaluación de riesgos e informes. Dicho sistema lógico (art. 20) se integra por un «conjunto de herramientas de *software* y la infraestructura de servidores y bases de datos», el «conjunto de datos» y los «mecanismos de análisis de datos, a través de indicadores de riesgo». Para la propia Generalitat Valenciana (contestación pregunta 6.ª) «en la actualidad, se puede considerar al sistema de alertas (SALER) como un sistema de análisis de datos, en el que se utilizan herramientas de BI [*business intelligence*], así como otras tecnologías más recientes como las bases de datos orientadas a grafos». Se está experimentando con herramientas como Big Data Analytics y existe voluntad de incorporar «inteligencia artificial», por ejemplo, para el análisis de relaciones entre entidades, pero estas cuestiones se abordarán en una fase posterior, cuando se consiga integrar la información de los sistemas corporativos.

La Generalitat Valenciana considera que no queda sometido a las exigencias de las decisiones solo automatizadas del artículo 22 del RGPD ni del artículo 41 de la Ley 40/2015. Así, se subraya que «la aplicación no toma ningún tipo de decisiones, ni mucho menos basadas únicamente en el tratamiento automatizado». De igual modo se considera (contestación pregunta 7.ª) que «el sistema SALER es una herramienta informática que no se incardina en ningún procedimiento administrativo sino que, […] la información que genere puede servir de base para tomar decisiones, como puede ser abrir unas diligencias previas de investigación o, en el caso de actuar otros órganos diferentes a la inspección y así tenerlo previsto, iniciar el correspondiente procedimiento administrativo. También puede aportar información que justifique realizar alguna actuación de mejora de la calidad de los servicios públicos».

---

[7] Así, ante la Dirección General de Planificación Estratégica, Calidad y Modernización de la Conselleria de Justicia, que fue resuelto favorablemente el 20 de agosto (GVRTE/2020/1163199). Se formularon 17 preguntas. He dispuesto un acceso a la resolución que incluye las preguntas formuladas en: <https://bit.ly/37f2apR>.

Hoy por hoy se trata de un sistema de baja actividad y capacidad: «No se ha instruido expediente sancionador alguno, ya que no se han detectado acciones u omisiones tipificadas como infracción por el artículo 41 de la Ley 22/2018» (contestación pregunta 2.ª). «Hasta la fecha no se ha iniciado ninguna actuación de investigación de irregularidades como consecuencia de análisis de datos efectuado en el sistema de alertas, aunque el sistema sí que se ha utilizado para obtener datos de utilidad con la finalidad de comprobar su funcionamiento mediante un análisis sobre contratos menores o para una actuación ordinaria sobre gestión de ayudas y subvenciones» (contestación pregunta 4.ª)[8]. «Aunque el sistema está implantado y operativo, se ha puesto en marcha con funcionalidades básicas, ya que tiene un carácter incrementalista» (contestación pregunta 3.ª). La Inspección cuenta con 10 puestos de inspectores si bien «en relación con el sistema de alertas, en la actualidad únicamente está siendo utilizado por un inspector, que es el responsable del desarrollo del proyecto» (contestación pregunta 14.ª).

3. TECNOLOGÍAS CONTRA EL FRAUDE SÍ, PERO CON GARANTÍAS JURÍDICAS

3.1. **Las tecnologías y la IA en principio son buenas para perseguir el fraude, pero con garantías**

En términos generales no parece cuestionable jurídicamente el uso de sistemas informáticos, automatizados, de *big data* o inteligencia artificial para el cumplimiento de la ley y la lucha contra el fraude.

En el caso holandés, se considera legítima la finalidad (6.3): «se deben utilizar esas nuevas posibilidades tecnológicas para prevenir y combatir el fraude» (6.4), es un «propósito suficientemente convincente para justificar una interferencia con la vida privada». De hecho, se califica como una «necesidad social imperiosa» («pressing social need») en términos del CEDH, lo cual legitima en abstracto la restricción de derechos. De hecho, se cuantifican los 2.000 millones de posible fraude que afectan a «la integridad del sistema económico y la confianza en las instituciones financieras» (6.76). Afirma que

[8] En este sentido se remite a la información más concreta de actuaciones en fichas resumen «rendición de cuentas».

<http://www.justicia.gva.es/es/web/planificacion-estrategica-calidad-y-modernizacion/inspeccion-de-servicios>.

«el uso de perfiles de riesgo en relación con el ejercicio de su deber regulatorio no es contrario al artículo 8.2 CEDH per se» (art. 6.102).

En el caso francés, el sistema está legitimado porque se «persiguió así el objetivo de valor constitucional de la lucha contra el fraude y la evasión fiscal» (n.º 84), se admite el «fin de investigar determinadas infracciones y determinadas infracciones cuya comisión sea posible o favorecida por el uso de Internet» (n.º 85). El Consejo Constitucional recuerda que le corresponde al legislador asegurar la conciliación entre el objetivo de valor constitucional de la lucha contra el fraude y la evasión fiscal y el derecho al respeto de la vida privada.

En esta dirección, respecto del sistema valenciano SALER, el informe AEPD 385661/2017 de marzo (AEPD, 2017) relativo al anteproyecto de la referida ley valenciana no duda en afirmar que «la finalidad del tratamiento (la lucha contra la corrupción, en un sentido amplio) sería admisible los *efectos* del artículo 23.1 RGPD» (AEPD, 2017: ap. IV), esto es, a los efectos de restricciones del derecho de protección de datos. Desde el punto de vista de este derecho señala que «prevenir irregularidades y malas prácticas», o por llamarlo de otro modo, ya que se cita la exposición de motivos, luchar contra el fraude y la corrupción, estaría incluido al menos en el apartado e), h) ó i) del apartado 1 del art. 23 RGPD. No obstante, esta finalidad parece perder algo de legitimación para restringir derechos para la AEPD cuando «el sistema en realidad es un sistema de alertas preventivo o prospectivo y no parece justificado en el anteproyecto de ley unas limitaciones, en realidad supresión, del derecho fundamental a la protección de datos como las sostenidas en el texto sometido a informe».

Frente a las muchas reticencias —a veces reaccionarias— frente al uso público de la IA, hay que tener una disposición favorable y no obstaculizadora, pero firmemente garantista. Más que una enmienda a la totalidad, el diablo está en los detalles y corresponde al jurista velar por ellos. Desde la Red Derecho Administrativo de la IA (DAIA) desde 2019 hemos subrayado elementos básicos jurídicos respecto del uso de la IA en el sector público que sin duda constituyen un referente. Así en las Conclusiones de Toledo de 1 de abril (Red DAIA, 2019*a*) y la Declaración final de Valencia de 24 de octubre (Red DAIA, 2019*b*) o las importantes aportaciones en la consulta de derechos digitales de julio (Red DAIA, 2020*a*) y especialmente el completo estudio de diciembre (2020*b*). De igual modo, cabe seguir las exigencias de buena administración, debido proceso y otros derechos señalados en los estudios de miembros de la Red como Cerrillo (2019), Ponce (2019), Valero (2019) o quien suscribe (2020), así como Boix (2020*a*) o Huergo (2020).

Respecto del uso público de IA, frente a la tolerante decisión en Estados Unidos en el caso *State vs. Loomis*, 881, N.W.2d 749, 7532 (Wis, 2016, ver

De Miguel 2018), en Europa se detectan mayores cautelas y restricciones, que entre otros ha analizado Boix (2020*a*). Así, entre otras, cabe recordar la Decisión N.º 2018-765 DC, 12 de junio de 2018 del Consejo Constitucional francés[9] o la Decisión 2019-796 DC de 27 de diciembre que se va a comentar, o Decisiones 2270/2019, 8472/2019 y 30/2020 del Consejo de Estado italiano. En general, no se trata de prohibiciones absolutas del uso de la IA (que sí que las hay para su uso judicial), sino de la necesidad de particulares garantías.

A falta de mejores normativas e interpretaciones jurisprudenciales, el derecho de protección de datos sigue absorbiendo el tratamiento jurídico del uso de la IA también en el sector público. Como he tenido ocasión de exponer (Cotino, 2019), por regla general el uso de IA respecto de personas supone un tratamiento de datos y, por tanto, sometido a la normativa general de protección de datos que implica muchas exigencias (minimización de datos, privacidad en el diseño y por defecto, delegados de protección de datos obligatorios en el sector público, tratamiento que por ser el sector público ha de venir legitimado a través de una ley, garantía de derechos, transparencia y acceso a la información del tratamiento, seguridad informática, análisis de riesgos *casi por defecto* será exigible un estudio de impacto).

Además, cuando se trata de exclusivamente decisiones automatizadas y con relevancia para las personas del artículo 22 RGPD, a las garantías del régimen general de protección de datos se añaden mayores garantías de transparencia (art. 13.2.º f y 14.2.º g), explicabilidad de la lógica del algoritmo, posibilidad de recurso e intervención y revisión humana de la decisión automatizada. El Grupo del artículo 29 (2018) y la AEPD (2020) van detallando estas garantías del cumplimiento normativo.

En febrero 2020 el Libro Blanco de la IA (Comisión Europea, 2020) adelanta la futura línea regulatoria, que implicaría la necesidad de un control previo de la IA de «alto riesgo», como sin duda lo es un tratamiento automatizado de grandes datos del sector público para la persecución del fraude. El Libro Blanco apuesta por garantías fuertes de seguridad, de calidad, solidez y exactitud de los datos, de conservación de registros de datos y trazabilidad, de transparencia e información y necesidades de supervisión y vigilancia. Y la Comisión propone generalizar un sistema de control previo de estas garantías para los sistemas de alto riesgo para verificar y garantizar su cumplimiento. En esta línea, la Carta iberoamericana de innovación en la gestión pública (CLAD, 2020) aboga por la aprobación «por una comisión

[9] <https://www.conseil-constitutionnel.fr/en/decision/2018/2018765DC.htm>.

multidisciplinar que valore si responde a la ética y a los valores públicos» y una «prueba de estrés de ética pública en una fase piloto y conseguir la acreditación de una agencia pública independiente», con «procedimientos sólidos pero sencillos y fluidos» (cap. 8.º, n.º 32).

A la espera de mejores regulaciones, al régimen de protección de datos, para el sector público hay que añadir en España el artículo 41.1.º Ley 40/2015 sobre actuaciones automatizadas. Sus insuficiencias son mayúsculas: solo establece algunas garantías previas, ciertamente escasas[10] y las reserva al uso en el marco formal de procedimientos administrativos, que además ha de ser «íntegramente» automatizado y sin supervisión humana.

3.2. **El uso de IA y *big data* en el sector público no puede huir de la aplicación del Derecho**

Se han mencionado esencialmente las garantías jurídicas, especialmente procedentes del régimen de protección de datos. No obstante, en este punto, hay que advertir que uno de los mayores peligros, es el que lo que he llamado la «huida del Derecho administrativo del uso de inteligencia artificial en el sector público» (Cotino 2020*b*).

Este fenómeno se da particularmente respecto del uso de la IA en las fases previas o de asistencia a las decisiones humanas. En nuestro caso, sistemas automatizados, tratamientos de grandes datos o inteligencia artificial se emplean para seleccionar supuestos de posible incumplimiento, potencial inspección, sanción u otras actuaciones. En cierto modo, el procedimiento y actuación individualizada ulterior sobre el sujeto es formalmente humano, puesto que el sistema automatizado solo ha preseleccionado el positivo.

Sin embargo, el sistema automatizado o algoritmo sí que influye en el contenido de la posterior acción administrativa, no en vano es la premisa de la actuación y posiblemente delimita los elementos estructurales básicos de la misma al detectar los patrones y pautas de la comisión de alguna irregularidad. Por decirlo de otro modo, para quien finalmente es sancionado, no es de escasa relevancia jurídica haber sido preseleccionado como posible infractor. Y, del contrario, no ser seleccionado y librarse de una actuación que sí que pueda corresponder, también es bien relevante. En modo alguno

---

[10] «[D]eberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación».

puede liberarse de garantías y obligaciones jurídicas considerando que se trata de actuaciones sin relevancia, o meramente auxiliares o complementarias y, obviamente, no se trata en ningún caso de actos meramente reglados automatizables que no hubieran de tener trascendencia jurídica[11].

Como se ha señalado, hoy día es especialmente difícil conocer los sistemas de IA que se están usando para asistir o apoyar decisiones públicas, especialmente en fases previas o preparatorias. Ello queda en general bajo el régimen parco y difuso de la «información y actuaciones previas» del artículo 55 Ley 39/2015 de procedimiento. En esta fase, la luz de la transparencia es muy tenue y difícilmente alcanza ni el derecho de acceso al expediente del propio interesado (artículo 53 Ley 39/2015) ni la legislación de transparencia (Boix 2020*b*). Además, como se ha visto respecto de la Agencia Tributaria, estos sistemas informáticos son «reservados» y quedan prácticamente blindados al control judicial. Este tipo de usos quedan fuera de la actuación formal y por ello se facilita una huida del Derecho y no se aplican las debidas garantías de transparencia, respeto del derecho a una buena administración, garantías del procedimiento, etc. Cabe recordar a este respecto que la sentencia de la Haya analiza y proyecta las garantías respecto de estos tratamientos automatizados que sirven para detectar un posible positivo. En modo alguno se entendió que no se trataba de una actuación administrativa plenamente fiscalizable y respecto de la que hay que exigir el cumplimiento de las garantías, antes al contrario, el sistema implicaba un «efecto legal, o al menos una decisión que afecta significativamente a los interesados» (6.57). Este debe ser el punto de vista de partida del legislador que debe regular estas fases.

Es por ello que debe haber una clara trazabilidad y transparencia del uso de sistemas algorítmicos en cualquier fase y tipo de actuación administrativa —formal o informal— que, entre otras cosas, permita determinar el grado real de intervención humana en la toma de decisiones (Red DAIA, 2019*b*: n.º 3.º).

3.3. **Hay que tomar nota de las muchas garantías mínimas exigidas en el caso holandés o del francés**

La regulación holandesa del sistema SyRI, pese a que fue declarada contraria a derechos fundamentales, era muy rigurosa e incluía muchas garantías

[11] Al respecto ver las aportaciones de Red DAIA en 2020 o Huergo (2020: 67 y ss.), si bien es posible discrepar de la falta de relevancia de algunas actuaciones que señala el autor. Ver también las aportaciones de Cotino y Huergo en el Observatorio de Transformación Digital del Sector Público: <https://t.co/1UvOSkGl8G?amp=1> <https://links.uv.es/P0TbuNz>.

de las que tomar muy buena nota. Y eso que eran para una fase de actividad que en España parece inmune a la exigencia de publicidad, garantías y control jurídico.

Una premisa esencial es la posibilidad de hacer una «fishing expedition», esto es, hacer rastreos indiscriminados para ver a quién se puede incriminar. Pues bien, en el caso holandés se parte de que en modo alguno cabe hacer rastreos indiscriminados con los sistemas automatizados. Por el contrario, legalmente estaba configurado bajo el principio de «seleccionar antes de recolectar» (4.23). Así, el sistema contaba con importantes garantías para evaluar la necesidad de aplicación de SyRI. Para solicitar el uso del sistema había requisitos específicos (4.20 y ss. secc. 65), se fijaba quién podía solicitarlo, demostrar la aprobación de uso dentro de cada organización, fijar qué datos serían necesarios y para qué «objetivo concreto», así como la «fecha de inicio prevista y la duración». Había de darse una evaluación individual de la necesidad y «haber comprobado por separado que el daño potencial a los intereses de las personas físicas o jurídicas … no es desproporcionado» (6.25).

La garantía de la confidencialidad (4.8) estaba regulada para todos los que accedieran a la información del sistema (4.16).

Otra garantía básica es que se anonimizan los datos y quienes acceden a los mismos no tienen la capacidad de vincularlos e identificar personas concretas. En el sistema SyRI, en una primera fase el órgano *Stichting Inlichtingenbureau* recopila datos, los seudonimiza y SyRI hace una primera selección de sujetos de riesgo. Los datos de los no seleccionados se destruyen en cuatro semanas y los datos de sujetos perfilados se descifran con el archivo de clave y son enviados al Ministerio. En esta segunda fase se analizan los perfiles más de cerca por la Inspección de Asuntos Sociales y Empleo (4.29). Los que no son seleccionados definitivamente son destruidos (4.31). Las referidas destrucciones se valoran positivamente en la sentencia, pero no son suficientes (6.81 y 6.92), esencialmente porque «la forma en que se lleva a cabo la selección definitiva del riesgo no es pública». Por cuanto a la destrucción, en cuatro semanas se borraban todos los *negativos* —no seleccionados como potenciales defraudadores— de la primera fase. Y respecto de los *positivos*, el tiempo máximo de uso y conservación del informe de riesgos estaba limitado a dos años y no de modo libre, sino con retroalimentación (4.15).

Resulta también de interés señalar que el Tribunal tampoco confía en la división funcional entre unidades administrativas: «El tribunal no puede evaluar si, y en qué medida, la división funcional interna entre […] la unidad

de investigación, la unidad de análisis y posiblemente otras unidades) está suficientemente protegida» (6.101).

Respecto de las auditorías externas e independientes, pese a que el tribunal valoró muchas de estas medidas, echó en falta «una revisión exhaustiva de antemano [y] una revisión por un tercero independiente […] con el fin de evaluar si es necesaria o no la restricción de derechos (6.99, y 96)».

Por cuanto a la necesidad de una evaluación de impacto (art. 35.10 RGPD) el tribunal señaló que pese a que no era obligatorio que hubiera servido para compensar la falta de «garantías insuficientes» (6.106), por lo que su ausencia vulnera el artículo 8.2 CEDH, no el RGPD.

El sistema experimental de la *Loi de finances* francesa para 2020 se consideró constitucional porque el legislador es el que pondera los derechos e intereses en juego y ha de brindar garantías suficientes y sí que tuvo en cuenta toda una serie de elementos, de los que también cabe tomar buena nota (n.º 87-93).

El Consejo Constitucional no fue tan exigente como el tribunal holandés, sin embargo, no son pocas las garantías de las que tomar nota:

Sí que se admitió la recopilación y tratamiento de datos procedentes de plataformas o servicio de comunicación en línea, siempre que el contenido sea «claramente hecho público por los usuarios de estos sitios», «solo se puede recopilar y utilizar el contenido relacionado con la persona que lo ha divulgado deliberadamente»; «por lo que se excluye el contenido accesible solo después de ingresar una contraseña o después del registro» (n.º 87). Ello no obstante, es cuestionable en España.

El Consejo Constitucional no admite incluir ningún sistema de reconocimiento facial (n.º 88).

El tratamiento solo puede hacerse «por agentes de las administraciones tributaria y aduanera que tengan al menos rango de controlador [responsables de tratamiento] y estén especialmente autorizados» (n.º 88).

Solo puede subcontratarse «el diseño de las herramientas de procesamiento de datos, con exclusión de su recolección, procesamiento y almacenamiento, podrá confiarse a un subcontratista de administración». Y en todo caso, «las personas que contribuyan al diseño y ejecución de las operaciones de tratamiento de que se trate están sujetas al secreto profesional» (n.º 88).

Por cuanto a los tiempos de destrucción de datos, «los datos que manifiestamente no guarden relación con los incumplimientos e infracciones buscados o que constituyen datos sensibles se destruyen a más tardar dentro

de los cinco días siguientes a su recogida, sin ningún otro uso posible de estos datos durante este período».

«Los demás datos deben destruirse en un plazo de treinta días si no es probable que contribuyan a la observación de las violaciones o infracciones. Solo podrán conservarse los datos estrictamente necesarios para tal constatación, en el plazo de un año o, en su caso, hasta que finalice el procedimiento penal, fiscal o aduanero en el contexto en que se utilicen» (n.º 89).

Mediación humana: si se da un positivo, es precisa una evaluación individual y no puede basarse exclusivamente en los resultados del sistema automatizado. Si se dan indicios de que una persona pudo haber cometido uno de los delitos o una de las infracciones buscadas, los datos recopilados se transmiten al departamento competente de la Administración para su corroboración y enriquecimiento. No se puede iniciar ningún procedimiento penal, fiscal o aduanero sin una evaluación individual de la situación de la persona por parte de la Administración, que luego no puede basarse exclusivamente en los resultados del procesamiento automatizado (n.º 90). A las garantías anteriores hay que añadir el posible ejercicio de los derechos de la protección de datos de acceso, rectificación, supresión, etc. (n.º 91).

4. LAS IMPORTANTES CARENCIAS DEL SISTEMA VALENCIANO SALER DESDE LA PROTECCIÓN DE DATOS Y LA FALTA DE CALIDAD DE LA LEY

No son suficientes las garantías desde la protección de datos, máxime siendo que la AEPD en su informe 385661/2017 de marzo sobre el anteproyecto de ley (AEPD, 2017) muy crítica —quizá en exceso— sobre la constitucionalidad del mismo.

Por cuanto al acceso a datos y división funcional, es cierto que la Generalitat Valenciana (pregunta 10), se indica que «al sistema solo tiene acceso personal el inspector de la Inspección General de Servicios. Además, la decisión de abrir una investigación sobre una persona física o jurídica se lleva a cabo fuera del sistema, sin que quede constancia de ello en la herramienta informática». Asimismo, en la respuesta a la cuestión 14.ª se añade que «para garantizar la confidencialidad de las personas relacionadas con la actuación inspectora, el acceso a los archivos y registros de la inspección queda restringido a dicho personal inspector y al personal de apoyo, que actualmente lo conforman dos personas. El sistema informático garantiza el control de accesos y permite realizar controles para verificar el correcto funcionamiento del sistema de acceso restringido». No obstante (respuesta 1.ª),

«tanto los órganos de control interno como externo podrán acceder a información del sistema SALER en el marco de las relaciones de colaboración y cooperación previstas en el Título I de la citada Ley».

La AEPD (2017: ap. II) criticó severamente la amplitud de los datos a tratar. Además reprueba que no se «distingue entre las distintas categorías de datos personales que pueden tratarse en dichas operaciones de tratamiento, puesto que el anteproyecto de ley es tan amplio y se refiere a un conjunto indeterminado de datos de los cuales no todos necesariamente tendrán la misma importancia». En su valoración en conjunto, la AEPD considera muy posible que el tratamiento de datos de SALER (2017: ap. III) sea desproporcionado, y especialmente la falta de claridad de la ley al respecto es llamativa. Y el exceso de datos a manejar queda al margen del conocimiento de los interesados incluso de su posible rectificación (AEPD, 2017: ap. III). También la AEPD (AEPD, 2017: ap. II) censura que se protejan más los datos del denunciante que los del denunciado que goza de presunción de inocencia. En conclusión, estas críticas, la multiplicidad de fuentes y la falta de calidad de la regulación llevan a afirmar la inconstitucionalidad de la ley y en su caso de los tratamientos que se hagan a su amparo.

Según diversos apartados de la ley, la inspección de servicios podrá acceder y recabar cuantos antecedentes, expedientes y documentación considere útiles para su cometido y cualquiera que sea su soporte (art. 7. 2.º c). Ello llevaría a tratar todo dato de quienes «tengan o hayan tenido una relación directa con la Administración de la Generalitat y su sector público instrumental referidos a expedientes administrativos relacionados con la contratación, con ayudas o subvenciones públicas, así como de las personas o entidades que mantengan o hayan mantenido una relación laboral o contractual con la Administración de la Generalitat y su sector público instrumental» (art. 17.3.º).

La AEPD (2017: ap. III) no admite que estos datos que la Administración tiene para otras finalidades, se desvíen para «la verificación o investigación de posibles irregularidades administrativas». Directamente considera que contrario al contenido esencial y a la STC 17/2013, de 31 de enero, la «LOPD no permite la comunicación indiscriminada de datos personales entre Administraciones Públicas competencias distintas o que versen sobre materias distintas de aquellas que motivaron su recogida, únicamente será posible si existe previsión legal expresa para ello (art. 11.2.a)». Y se considera que aunque la nueva finalidad está fijada por la ley valenciana, «el rango legal es condición necesaria, pero no suficiente», pues «en todo caso ha de respetar el contenido esencial del derecho fundamental (art. 53.1 CE)». Es más, el artículo 19 de la Ley 22/2018 valenciana, permite integrar datos que por

obligación de colaboración con la Generalitat Valenciana faciliten terceros, obligados sobre contratistas, subvencionados y trabajadores investigados. Y ello solo bajo condición de que la procedencia de estos datos de los terceros sea legítima. La AEPD (2017) también considera «desproporcionada» esta exigencia, que va más allá del deber de colaboración del artículo 18 de la Ley 39/2015. La AEPD censura que se hace, además, «sin que el interesado tenga siquiera conocimiento de la utilización de dichos datos personales para finalidades distintas de las propias para las que se aportaron. se le privaría también del derecho de rectificación de dichos datos».

En cualquier caso, pese a que la ley posibilite toda esta amplia gama de datos, la Generalitat Valenciana afirma (respuesta 12.ª) que «en la actualidad se utilizan las siguientes bases de datos: Registro de Contrato, Registro de Ayudas y Subvenciones, información relacional obtenida del BORME, registro de control de conflicto de intereses». Se prevé «la incorporación de la información proveniente de las propias aplicaciones corporativas de gestión, con lo que el nivel de información será mucho mayor y permitirá una mayor explotación del sistema» (respuesta 3.ª).

Según se ha visto, la ley francesa sí que permite el manejo de datos de plataformas y redes sociales. El artículo 17.3.º de la ley valenciana también permite integrar datos de todos estos contratistas, subvencionados o trabajadores que «hayan hecho manifiestamente públicos de manera voluntaria, particularmente en internet» (en páginas indexables, redes abiertas y que no sean íntimos). Hoy por hoy la Generalitat Valenciana afirma (respuesta pregunta 12.º) que «en cuanto al artículo 17.3, no se está utilizando información procedente de ninguna red social». La AEPD (2017: ap. II) critica especialmente el uso de datos de internet «sin que el interesado tenga siquiera conocimiento de la utilización de dichos datos personales para finalidades distintas de las propias para las que se aportaron, se le privaría también del derecho de rectificación de dichos datos».

La reciente STC 27/2020, de 24 de febrero no parece ir en la línea de admitir el tratamiento de datos procedentes de redes y plataformas pese a que sean accesibles: «salvo excepciones tasadas, por más que los ciudadanos compartan voluntariamente en la red datos de carácter personal, continúan poseyendo su esfera privada que debe permanecer al margen de los millones de usuarios de las redes sociales en internet, siempre que no hayan prestado su consentimiento de una manera inequívoca para ser observados o para que se utilice y publique su imagen» (FJ 2.º) «el usuario de Facebook que “sube”, “cuelga” o, en suma, exhibe una imagen para que puedan observarla otros, tan solo consiente en ser observado en el lugar que él ha elegido (perfil, muro, etc.)».

Ahora bien, no puede excluirse que la ley regule esta posibilidad de tratamiento de información en razón de funciones e intereses públicos [art. 6.1.º e) RGDP]. No obstante, sin duda se requiere una ley de calidad que determine no solo la posibilidad de la restricción, sino que ha de contener disposiciones específicas sobre la finalidad y tipo del tratamiento, las categorías de datos concretos que se van a tratar y el alcance de restricciones. Y, sobre todo, la ley ha de regular las garantías y derechos específicos de los afectados y otros elementos como la precisión de plazos de conservación. Ello es así en razón de las exigencias constitucionales, especialmente a partir de la STC 76/2019 (que declaró inconstitucional la regulación orgánica que permitía el perfilado de datos ideológicos en las redes por partidos políticos), así como de las exigencias del artículo 23 RGPD. Ciertamente la ley valenciana no contiene estos elementos y es difícilmente aceptable.

Por cuanto al ejercicio de derechos por los afectados, se preguntó a la Generalitat Valenciana (pregunta 9.ª) específicamente «si el sistema tiene previsto facilitar información respecto de las personas que hayan sido de algún modo analizadas pero no investigadas». Según se ha visto, ello fue muy importante para la conclusión de violación de derechos en el caso holandés y un elemento positivo para la constitucionalidad de la ley francesa. Al respecto, la respuesta que brinda la Generalitat Valenciana es difusa: si se diese una actuación de investigación se brindaría la información necesaria y limitada. De tal respuesta se infiere que los investigados no seleccionados, no serán objeto de derechos. A este respecto, la AEPD critica que «dicha medida legislativa no contiene una disposición específica sobre el derecho de los interesados a ser informados».

Otro foco de críticas importante de la AEPD (2017: aps. III y V) es el excesivo plazo de conservación de los datos. Cabe recordar la rápida destrucción de los datos en los casos holandés y francés. Sin embargo, en el anteproyecto valenciano se hablaba de diez años y también se contemplaba la conservación de los datos y sin anonimizar más allá del plazo de prescripción de las irregularidades. Para la AEPD ello es una «grave intrusión», «la regulación que al respecto se contiene en el anteproyecto de ley es excesiva e infringiría el principio de limitación del plazo de conservación contenido en el art. 5.1.e) del RGPD». La ley finalmente aprobada menciona una conservación de ocho años en su exposición de motivos. Sin embargo, en el articulado, de un lado, el artículo 36 habla en general del adecuado archivo y la disp. adicional 3.ª 4.º simplemente señala que se conservarán los datos «durante el tiempo imprescindible». No resulta admisible la no fijación de plazos o al menos elementos para su determinación concreta. Y en todo caso, el plazo de ocho años mencionado sería inadmisible. La Generalitat Valenciana al respecto (respuesta pregunta 11.ª) viene a decir que no hay una regulación

específica de la conservación de los datos del sistema de alertas. Señala por otra parte que «la previsión reglamentaria es que la documentación que forme parte del archivo de la actuación conserve su contenido original», si bien menciona genéricamente la posibilidad de anonimización.

5. «BLACK BOX»: LA FALTA DE TRANSPARENCIA E INFORMACIÓN QUE TAMBIÉN VIOLA DERECHOS DE DEFENSA Y NO DISCRIMINACIÓN, TAMBIÉN EN EL CASO VALENCIANO

Un elemento esencial de garantía frente al uso de la IA en el que hemos insistido desde la Red DAIA (por ejemplo, 2019*a*: n.º 9 y especialmente 2020*b*) son las obligaciones de transparencia, auditabilidad y explicabilidad del algoritmo, abogamos por «la transparencia y justificación desde el diseño que genere datos auditables». Se precisan sistemas «white box» frente a la *caja negra*. Estas exigencias derivan de diversos derechos fundamentales como el derecho de acceso a la información, el debido proceso y las garantías judiciales y administrativas, el derecho a la buena administración, así como principios como la interdicción de la arbitrariedad y la rendición de cuentas. Además de estos derechos, es una exigencia del derecho a la protección de datos que implica transparencia y derecho de acceso a la información. Y si además se aplica el artículo 22 RGPD para decisiones automatizadas, se refuerzan estas obligaciones de acceso, transparencia y explicabilidad, lo mismo que el control y las auditorías en el caso de ser aplicable el artículo 41 Ley 40/2015.

Pues bien, en el caso holandés, además de la falta de independencia y de auditorías y de la ingente cantidad de datos personales que se manejaban, la carencia más grave para la sentencia y que lleva a considerar que las muchas garantías fueran insuficientes son los problemas de caja negra y opacidad de SiRY así como la falta de información a los interesados cuyos datos se tratan. La sentencia afirma que «el principio de transparencia es el principio principal de protección de datos» (6.87). En el famoso caso *State v. Loomis*, 881, N.W.2d 749, 7532 (Wis, 2016), la aplicación de algoritmos predictivos determinó el incremento de la pena por la peligrosidad. En aquel supuesto, desde el debido proceso el tribunal consideró suficiente la información facilitada a la defensa —poco más que un manual de la aplicación— al tiempo que señalaba que los propios jueces garantizaban suficientemente los derechos de la defensa en la aplicación concreta. En el caso holandés el tribunal concluye que la «legislación SyRI es insuficientemente transparente y verificable» (6.86); no hay «garantías insuficientes» de transparencia (6.95).

El Estado holandés solo informó de que el modelo de riesgo consiste en i) indicadores de riesgo, ii) enlaces y iii) el denominado punto de corte. Se argumentaba que se utilizaban modelos «validados» por la autoridad, con indicadores de riesgo verificados por la experiencia. No se quería dar más información precisamente para evitar prácticas o tecnología inversa por posibles defraudadores que les permitiera eludir ser considerados perfiles de riesgo a inspeccionar: «La razón que da el Estado para esto es que los ciudadanos podrían ajustar su conducta en consecuencia. Esta es una elección deliberada del Estado» (6.49). Sin embargo, el tribunal no lo admitió porque «no permite conocer la validación del modelo de riesgo y la verificación de los indicadores» por lo que «resulta imposible verificar cómo se genera el árbol de decisión» (6.89). Se señala que «es difícil comprender cómo un interesado podría defenderse contra el hecho de que se haya presentado un informe de riesgos sobre él o ella» (6.90).

Por cuanto a la opacidad del sistema la sentencia afirma que «el modelo de riesgo que se está utilizando actualmente y los indicadores de riesgo que constituyen este modelo de riesgo son "secretos" […] ni son conocidos por los interesados» (6.65). El sistema «de ninguna manera proporciona información sobre los datos fácticos que pueden demostrar la presencia de una determinada circunstancia […] datos objetivos que pueden justificar la conclusión de que existe un mayor riesgo» (6.87). «El Estado no ha explicado en qué información objetivamente verificable se basan estos ejemplos» (6.88) y «no proporciona información sobre el funcionamiento del modelo de riesgo y el tipo de algoritmos […] ni […] sobre el método de análisis de riesgos aplicado» (6.89).

También la sentencia ataca la falta de transparencia e información sobre los tratamientos de datos a los interesados. La legislación no establece la obligación de notificar a los interesados individualmente «puerta a puerta» (6.53). Además, quienes no son considerados perfil de riesgo, no pueden saber cómo se procesaron sus datos. Que deban destruirse los datos en estos casos a las cuatro semanas, «no altera el requisito de transparencia con respecto a ese procesamiento» (6.89). Los interesados «tampoco son informados automáticamente después», sino que solo se les informa si hay un control e investigación en respuesta a un informe de riesgos (6.53).

Desde la igualdad y no discriminación también se afirma que «la transparencia, en aras de la verificabilidad» es necesaria frente a los peligros de «exclusión o discriminación injustificadas» (6.91). De hecho, los demandantes y el Relator Especial de la ONU consideraban que SyRI «tiene un efecto discriminatorio y estigmatizador», pues al investigar vecindarios más marginados, «contribuye a los estereotipos y refuerza una imagen negativa de los

ocupantes de dichos vecindarios». Ello sería admisible si se conociese el sistema y se pudiera neutralizar este riesgo, pero como no se conoce cómo se lleva a cabo la segunda fase de selección definitiva del riesgo, el sistema es discriminatorio por falta de transparencia (6.92). Se trataría de saber hacia dónde pone el foco el algoritmo para no «criminalizar la pobreza» centrándose en el posible cobro de prestaciones indebidamente y no centrarse en la falta de pago de cotizaciones, por ejemplo (Todolí, 20202: 328).

Frente a estas proclamaciones de la necesidad de transparencia Todolí (2020: 329-330) en la línea de Boix (2020*a*: 265) señala que no debe incluirse en esa 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. Hay motivos para la reserva. Así, informar a las empresas de que tienen una baja probabilidad de ser investigadas podría incrementar el propio incumplimiento. Igualmente, publicar el código o las ponderaciones realizadas por la herramienta para tomar la decisión permitiría que los posibles inspeccionados pudieran tener información de las posibilidades concretas de ser inspeccionadas. También, 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 y no para cumplir con la norma, sino modificar esas variables (lo que se ha llamado *gaming the algorithm*). Admite al menos que 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) y la necesidad de auditorías internas o mejor externas e independientes.

En el caso valenciano, la AEPD (2017: VI) ya censuró que se considerase suficiente la sola publicación de la ley. Y ello porque a diferencia de casos como la STJUE de 1 de octubre de 2015, C- 201/14, Smaranda Bara, el contenido de la ley ha de permitir tomar conocimiento correcto y concreto de toda la información obligatoria por el artículo 13 RGPD. Y ello no es fácil a partir de la propia ley valenciana.

Expresamente se solicitó información como la que exige la AEPD (2020) en su guía sobre inteligencia artificial en razón de los artículos 22 y 13 RGPD[12]. Sin embargo, por un lado y en general, la Generalitat Valenciana

[12] Así, se solicitó información sobre la importancia relativa que cada dato de los empleados tiene en la toma de decisión; los indicadores de riesgo y el peso de cada uno de ellos, en su caso, así como el punto de corte para considerar un positivo por el sistema. Con relación al artículo 27 de la ley se solicita información de si ya existe el sistema de indicadores ahí referido y la codificación estandarizada. También se solicitó la descripción básica de dicho

considera que no se está utilizando inteligencia artificial ni se está en el marco del artículo 22 RGPD por lo que no aplican esas obligaciones de transparencia (respuesta 12.ª). No obstante, por otro lado se afirma que «los algoritmos que se utilizan actualmente, y los que se puedan utilizar en un futuro, pueden ser facilitados a quien los solicite, ya que se trata de "preguntas" sobre circunstancias concretas de los procedimientos administrativos de las áreas de gestión que se incorporen al sistema de alertas, como por ejemplo, "contratos realizados a un mismo adjudicatario por un mismo adjudicador, para un mismo objeto de contrato (CPV) en un período"».

Asimismo se solicitó informes de conclusiones y recomendaciones de cada actuación y los informes de evaluación del sistema (regulados en art. 17 d) de la Ley valenciana. A este respecto, la Generalitat Valenciana en su respuesta a la pregunta 13.ª reconduce la cuestión a los mapas de riesgos que dan lugar a las nuevas preguntas algoritmos al sistema y que están en fase de elaboración. Y en esta dirección se reenvía a una ficha resumen de conclusiones y recomendaciones de las actuaciones inspectoras y de los informes de evaluación.

Pues bien, la transparencia e información del sistema SALER es muy reducida. Poco se sabe del sistema más allá de la regulación legal y de la remisión a unos informes y actuaciones dudosamente vinculadas al desarrollo del sistema automatizado. Eso sí su nivel de uso y, en consecuencia, afectación concreta de derechos hasta el momento es muy limitado o nulo.

Y por cuanto la facilitación de derechos y en concreto de acceso a los datos del tratamiento por los posibles afectados, en modo alguno puede considerarse suficiente puesto que simplemente se dice que en su caso se remitiría información. Cabe recordar no solo las altas exigencias holandesas, sino que en el caso francés estos derechos estaban específicamente reconocidos.

Las nuevas tecnologías pueden permitir umbrales de eficacia contra el fraude y la corrupción hasta ahora desconocidos. No obstante, el Estado de derecho atempera necesariamente estas posibilidades y, especialmente, obliga a esforzarse mucho al diseñar los sistemas para el cumplimiento normativo.

---

sistema de indicador, si ha habido una actualización periódica de dicho sistema, la calidad de los datos de entrenamiento y el tipo de patrones utilizados, los perfilados realizados y sus implicaciones, los valores de precisión o error según la métrica adecuada para medir la bondad de la inferencia, la existencia o no de supervisión humana cualificada. También, las auditorías, especialmente sobre las posibles desviaciones de los resultados de las inferencias, así como la certificación o certificaciones realizadas sobre el sistema de IA. En el caso de sistemas adaptativos o evolutivos, la última auditoría realizada y si la auditoría es interna o externa y por que órganos o instituciones se ha hecho.

No hay que abandonar el camino que ya se está trazando, pero hay que dotarlo de las suficientes garantías que ya se van definiendo pese a la falta de un mejor marco regulatorio.

BIBLIOGRAFÍA

Autoritat Catalana de Protecció de Dades, ACPD (2020). *Intel·ligència Artificial. Decisions Automatitzades a Catalunya*. ACPD y Generalitat. URL: <https://apdcat.gencat.cat/web/.content/04-actualitat/noticies/documents/INFORME-INTELLIGENCIA-ARTIFICIAL-FINAL-WEB-OK.pdf>.

AEPC (2020). *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial. Una introducción*. febrero. URL: <https://www.aepd.es/media/guias/adecuacion-rgpd-ia.pdf>.

AEPD (2017). «Informe AEPD 385661/2017 de marzo relativo al anteproyecto de ley de sistema de alertas tempranas de la Comunidad Valenciana». [No publicado. He dipuesto un enlace en: <https://www.dropbox.com/s/utzo5hrkf0b3cmi/aepdantifraude.pdf?dl=0>].

Agencia Tributaria (2020). *Plan Estratégico 2020-2023* (2020). URL: <https://www.agenciatributaria.es/static_files/AEAT/Contenidos_Comunes/La_Agencia_Tributaria/Planificacion/PlanEstrategico2020_2023/PlanEstrategico2020.pdf>.

Arena, G. (1993). «Transparencia Administrativa y Democracia», en *Revista Vasca de Administración pública*, n.º 37, 1993, pp. 9-20. URL: <https://dialnet.unirioja.es/servlet/articulo?codigo=1166150>.

Ballart, X. y Ramió, C. (2000). *Ciencia de la Administración*. Valencia: Tirant lo Blanch.

Boix, A. (2020*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», en *Revista de Derecho Público: Teoría y Método*, vol. 1 (2020), pp. 223-270.

— (2020*b*). «Límites al derecho de acceso a la información pública en procedimientos de información y actuaciones previas», en Cotino, Lorenzo y Boix, Andrés (ed.): *Los límites al derecho de acceso a la información pública*, 2020, pp. 228-242. Valencia: Tirant Lo Blanch.

Brandeis, L. B. (1913). «What Publicity Can Do», en *Harper's Weekly*. URL: <http://goo.gl/dEbaI>.

Cerrillo, A. (2019). «El impacto de la inteligencia artificial en el Derecho administrativo, ¿nuevos conceptos para nuevas realidades técnicas?», en *Revista general de Derecho administrativo*, n.º 50.

CLAD (2020). *Carta iberoamericana de innovación en la gestión pública*, Conferencia Iberoamericana de ministras y ministros de la Administración Pública y Reforma del Estado, Andorra, 8 de octubre de 2020.

Comisión Europea (2006). *Risk Management Guide for Tax Administrations,* Bruselas. URL: <https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/taxation/tax_cooperation/gen_overview/risk_management_guide_for_tax_administrations_en.pdf>.

— (2020). *Libro Blanco sobre la inteligencia artificial — Un enfoque europeo para la excelencia y la confianza,* COM(2020) 65 final, Bruselas. 19.2.2020, [ver pp. 21 y ss.]. URL: <https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1>.

Cotino, L. (2013). «Del "deber de publicidad" de Brandeis al "open Governement" de Obama. Regulación y control de la información pública a través de las nuevas tecnologías», en Escobar Roca, Guillermo (ed.): *La protección de los derechos humanos por las defensorías del pueblo*, 2013, pp. 859-885. Madrid: Dykinson. Madrid. URL: <http://goo.gl/br3rs>.

— (2019). «Derecho y garantías ante el uso público y privado de inteligencia artificial, robótica y big data»: en Bauzá, Marcelo (dir.), *El Derecho de las TIC en Iberoamérica*, 2019, pp. 917-952. Montevideo: La Ley-Thompson-Reuters. URL: <http://links.uv.es/BmO8AU7>.

— (2020*a*), «"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», en *La Ley Privacidad, Wolters Kluwer* n.º 4, mayo 2020. URL: Academia.

— (2020*b*). «Garantías frente a la huida del Derecho administrativo del uso de inteligencia artificial en el sector público», en *Observatorio de la Transformación Digital Sector Público*. URL: <https://links.uv.es/vWpZkh7. URL: https://youtu.be/TT0Exq-eq80>.

Criado, J. I., Valero J. y Villodre J. (2020). «Algorithmic transparency and bureaucratic discretion: The case of SALER early warning system», *Information Polity 25* (2020) 449-470.

Curtin, D. M. (2000*b*). «Citizens' Fundamental Right of Access to EU Information: An Evolving Digital *Passepartout*?», en *Common Market Law Review,* 37, pp. 7-41.

De Miguel, I. (2018). «Does the use of risk assessments in sentences respect the right to due process? A critical analysis of the Wisconsin v. Loomis ruling», en *Law, Probability and Risk*, n.º 17, (1), pp. 45-53.

Dyrberg, P. (1999). «Current issues in the debate on public access to documents», en *European Law Review*, 24 (2), pp. 157-170.

Engstrom, D. F., Ho, D. E., Sharkey, C. M. y Cuéllar, M.-F. (2020). *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies*. DOI: <https://doi.org/10.2139/ssrn.3551505>.

Galetta, D.-U. (2017). «Trasparenza e contrasto della corruzione nella pubblica amministrazione: verso un moderno panottico di Bentham?», en *Diritto e Società*, vol. 1.

Gutiérrez David, María Estrella (2020). «Trazabilidad y explicabilidad de los algoritmos públicos», en Cotino Hueso, L. (dir.), *Observatorio de Transformación Digital del Sector Público*, <https://www.uv.es/fatwireed/catedra-pagoda/es/novedades-1286053802801/Novetat.html?id=1286162435736>.

Grupo del Artículo 29 (2018). *Directrices sobre decisiones automatizadas de 6 de febrero de 2018*. URL: <https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf>.

Huergo, A. (2020). «Una aproximación a los algoritmos desde el Derecho administrativo», en Huergo, A. (2020): *La regulación de los algoritmos,* pp. 23-88. Cizur: Aranzadi.

Misuraca, G. y Van noordt, C. (2020). *Overview of the use and impact of AI in public services in the EU*, EUR 30255 EN. Luxembourg: Publications Office of the European Union. DOI: <https://doi.org/10.2760/039619>.

OCDE, *OECD Regulatory Enforcement and Inspections Toolkit*. París, 2018. URL: <https://www.oecd.org/gov/regulatory-policy/oecd-regulatory-enforcement-and-inspections-toolkit-9789264303959-en.htm>.

Ponce, J. (2019). «Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico», en *Revista General de Derecho Administrativo* Iustel, n.º 50.

Red DAIA (2019*a*). *Conclusiones de Toledo de 1 de abril*. URL: <https://www.dropbox.com/s/5px5jkvauiz06vu/CONCLUSIONES_DAIAvfinal.pdf?dl=0>.

— (2019*b*). *Declaración final de Valencia de 24 de octubre*. URL: <https://www.dropbox.com/s/zlth1wq0n2z8c0b/DAIA_Valenciadeclaracion.pdf?dl=0>.

— (2020*a*). *Aportación a consulta de derechos digitales de julio.* URL: <https://www.dropbox.com/s/w9xlb64o1zemaca/DAIACONSULTAvenviada.pdf?dl=0>.

— (2020*b*). Cerrillo, Agustí; Gamero, Eduardo; Cotino, Lorenzo; Martín Delgado, Isaac; Ponce, Juli y Velasco, Clara, *Aportaciones de la Red DAIA a la carta de derechos digitales. Carta de Derechos digitales y sector público: propuestas de mejora*, Red DAIA. Diciembre 2020, <https://bit.ly/3paF0H0>.

Todolí, A. (2020). «Retos legales del uso del big data en la selección de sujetos a investigar por la Inspección de Trabajo y de la Seguridad Social», en *Revista Galega e Administración pública (REGAP)*, n.º 59, pp. 313-337. DOI: <https://doi.org/10.36402/regap.v0i59.4354>.

Valero, J. (2019). «Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración», en *Revista catalana de dret públic*, n.º 58, 2019, pp. 82-96.

Warren S. y Brandeis, L. D. (1890). «The Right To Privacy», en *Harvard Law Review,* 193. URL: <http://goo.gl/Le3oJ>.

Watkins, R. C. *et al*. (2003). «Tracking dirty proceeds: Exploring data mining technologies as tools to investigate money laundering», en *Police Practice and Research*, 4, pp. 163-178. DOI: <https://doi.org/10.1080/15614260308020>.

Wirtz, B. W., Weyerer, J. C. y Geyer, C. (2019). «Artificial Intelligence and the Public Sector—Applications and Challenges», en *International Journal of Public Administration*, 42 (7), pp. 596-615. DOI: <https://doi.org/10.1080/01900692.2018.1498103>.