UNA REGULACIÓN LEGAL Y DE CALIDAD PARA LOS ANÁLISIS AUTOMATIZADOS DE DATOS O CON INTELIGENCIA ARTIFICIAL. LOS ALTOS ESTÁNDARES QUE EXIGEN EL TRIBUNAL CONSTITUCIONAL ALEMÁN Y OTROS TRIBUNALES, QUE NO SE CUMPLEN NI DE LEJOS EN ESPAÑA

Por

LORENZO COTINO HUESO [1]
Catedrático de Derecho Constitucional de la Universitat de València. Investigador de la Universidad Católica de Colombia. Valgrai

Revistas@iustel.com

Revista General de Derecho Administrativo 63 (2023)

RESUMEN: La sentencia del Tribunal Constitucional alemán de 2023 ha anulado dos leyes que permitían la evaluación automatizada de datos con fines policiales. Además, establece elevados estándares de calidad de la ley para los tratamientos automatizados de datos para la prevención del delito. Asimismo, excluye el uso de sistemas IA. La regulación legal debe establecer los mínimos técnicos y organizativos y limitar los métodos y los datos utilizados. Esta importante sentencia se suma a una tendencia jurisprudencial exigente en Europa y España. Dadas las graves carencias legales en España, es imperativa la actuación de un legislador de calidad, incluso con el futuro Reglamento de la Unión Europea.

PALABRAS CLAVE: inteligencia artificial, tratamientos automatizados, protección de datos, derechos fundamentales, calidad de la ley.

SUMARIO: I. La necesidad de una respuesta del Derecho que acompañe los crecientes usos de los sistemas automatizados y con inteligencia artificial; II. Los presupuestos de la sentencia del tribunal constitucional alemán de 2023, que declara la nulidad de la evaluación o análisis automatizado de datos con fines policiales; III. Los elevados estándares de calidad de la ley que fija el Tribunal Constitucional alemán; IV. Esta sentencia se suma a una clara línea jurisprudencial exigente en Europa y España; V. Para concluir: la imperiosa necesidad de regulación de calidad en España, incluso con el futuro Reglamento de la Unión Europea.

---

[1] ORCID: 0000-0003-2661-0010. cotino@uv.es. OdiseIA. El presente estudio es resultado de investigación del proyecto “Derecho, Cambio Climático y Big Data”, Grupo de Investigación en Derecho Público y TIC; MICINN Retos “Derechos y garantías frente a las decisiones automatizadas... (RTI2018-097172-B-C21); “La regulación de la transformación digital …” grupo de investigación de excelencia Generalitat Valenciana “Algoritmic law” (Prometeo/2021/009, 2021-24); “Transición digital de las Administraciones públicas e inteligencia artificial” (TED2021-132191B-I00) y “Algorithmic Decisions and the Law: Opening the Black Box” (TED2021-131472A-I00), del Plan de Recuperación, Transformación y Resiliencia. Estancia Generalitat Valenciana CIAEST/2022/1. Última visita de urls 10 de abril 2023.

A LEGAL AND QUALITY REGULATION FOR AUTOMATED DATA ANALYSIS OR WITH ARTIFICIAL INTELLIGENCE. THE HIGH STANDARDS REQUIRED BY THE GERMAN CONSTITUTIONAL COURT AND OTHER COURTS, WHICH ARE FAR FROM BEING FULFILLED IN SPAIN

ABSTRACT: The increasing use of automated systems and artificial intelligence requires an adequate legal response. The German Constitutional Court ruling of 2023 annulled two laws that allowed automated data evaluation for law enforcement purposes. It sets high-quality standards of law for automated processing for crime prevention and excludes the use of AI and autonomous systems. The regulation must establish technical and organizational minimums and limit the methods and data that can be used. This important ruling is one more example of the demanding jurisprudential trend in Europe and Spain. Given the serious legal shortcomings in Spain, quality legislation is imperative, even with the future EU regulation.

KEYWORDS: artificial intelligence, automated processing, data protection, fundamental rights, quality of the law.

SUMMARY: I. The need for a legal response to the increasing use of automated and artificially intelligent systems; II. The assumptions of the German Constitutional Court's ruling of 2023, which declares the nullity of automated data evaluation or analysis for law enforcement purposes; III. The high standards of quality of law set by the German Constitutional Court; IV. This ruling is one more in the clear line of demanding jurisprudence in Europe and Spain; V. To conclude: the imperiousneed for quality regulation by law in Spain, even with the future EU Regulation.

I. LA NECESIDAD DE UNA RESPUESTA DEL DERECHO QUE ACOMPAÑE LOS CRECIENTES USOS DE LOS SISTEMAS AUTOMATIZADOS Y CON INTELIGENCIA ARTIFICIAL

Los usos públicos de los sistemas automatizados y especialmente la inteligencia artificial (IA) ya son de lo más variado, como los 600 casos de usos públicos en la UE analizados en 2022[2]. Se emplea *machine learning* para la detección de fraude, mejora de la calidad de los documentos, predicciones basadas en los datos disponibles, automatización de tareas repetitivas con capacidad de adaptación. También, tecnologías de IA de planificación y programación para la planificación y gestión en el sector público para impuestos, recursos, empleo, atención médica, energía, materiales y muchos más. Técnicas de Procesamiento del Lenguaje Natural para identificar, procesar, comprender o generar información en comunicaciones humanas escritas y habladas. Sistemas de visión automática así como de representación del conocimiento que previenen y

[2] Sobre los usos públicos de IA, JRC, Tangi, L. y otros, *AI Watch European landscape on the use of Artificial Intelligence by the Public Sector*, JRC Science For Policy Report, Unión Europea; OCDE, Ubaldi, Barbara y otros, *State of the art in the use of emerging technologies in the public sector*, OECD Working Papers on Public Governance No. 31, 2022; Freeman Engstrom, D. y otros, "Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies. Report submitted to the Administrative conference of the United States", *NYU School of Law, Public Law Research Paper No. 20-54* 2020. Asimismo, mi estudio, "Los usos de la IA en el sector público, su variable impacto y categorización jurídica" *Revista Canaria de Administración Pública*, nº 1, 2023.

predicen, permiten experimentar opciones públicas, mejoran los servicios y la información pública, automatizan tareas repetitivas. La IA y los sistemas automatizados ya son el *dedo* que nos preselecciona para ser inspeccionados, o directamente sancionados. Con IA se apoyan las decisiones políticas y administrativas y muy pronto las decisiones judiciales. Por lo general, cada uno de nosotros ni la sociedad civil sospechamos todo lo que ya se hace. Y no siempre podemos estar muy seguros de que el sector privado o público que utiliza la IA tiene un control y conocimiento pleno de estos sistemas lo que hace.

La IA, los sistemas automatizados y las tecnologías conexas pueden ser muy positivas para la sociedad y para los individuos. Es por ello por lo que el Derecho también tiene que proteger el desarrollo de la IA y acompañar e impulsar la innovación constante. No obstante, pese a las bondades de la IA, especialmente un jurista no puede desconocer que hay un lado mucho más oscuro. La autonomía es un elemento propio de la IA y de por sí es un peligro añadido a los muchos peligros e impactos que generan los sistemas que hagan tratamientos automatizados de datos[3] o que integren algoritmos, esto es, fórmulas más o menos complejas y las apliquen a los datos. Los hombres integrados en equipos y entidades que diseñan la IA no son *ángeles*. Involuntariamente pueden generar sistemas con errores y sesgos y por tanto con impactos estructurales en los principios constitucionales y los derechos fundamentales. Y, por supuesto, también los desarrolladores pueden ser voluntariamente *demonios*. Además, la IA y los sistemas autónomos con autoaprendizaje en cierto modo cobran cierta independencia de su diseñador y creador. Así las cosas, *estos sistemas autónomos tampoco son ángeles*, sino que pueden convertirse también en auténticos demonios. Como afirmara James Madison (El Federalista 51): "Si los hombres fueran ángeles, no sería necesario ningún gobierno. Si los ángeles gobernaran a los hombres no sería necesario ningún control ni externo ni interno sobre el gobierno". Trasladando esta afirmación al Derecho, no cabe duda de que el papel del Derecho es fundamental frente a los nuevos riesgos[4].

Recientemente publiqué el estudio "Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal"[5]. El propio

[3] Por todos, Palma Ortigosa, Adrián, *Decisiones automatizadas y protección de datos personales. Especial atención a los sistemas de inteligencia artificial*, Dykinson, 2022.

[4] "Riesgos e impactos del big data, la IA y la robótica y enfoques, modelos y principios de la respuesta del Derecho", Boix Palop, Andrés y Cotino Hueso, Lorenzo (coords.), *Monográfico Derecho Público, derechos y transparencia ante el uso de algoritmos, IA y big data RGDA Iustel*, nº 50, febrero 2019. Acceso en completo https://bit.ly/37RifyJ

[5] Cotino Hueso, Lorenzo, "Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal", en *El Cronista del Estado Social*, IUSTEL, monográfico Inteligencia artificial, nº 100, septiembre-octubre 2022, pp. 68-79. Una versión extensa de este estudio y con más referencias, "Reconocimiento facial automatizado y sistemas de

título clamaba por la necesidad de una buena regulación legal que nos permita utilizar estas tecnologías, pero con todas las garantías exigibles. En éste y otros estudios más detallados volcaba la atención en estos sistemas que suponen el tratamiento masivo de datos con sistemas automatizados y, en particular, con inteligencia artificial. Especialmente subrayaba que los sistemas automatizados, y más si cabe si cuentan con IA, suponen un salto cualitativo en el impacto a los derechos fundamentales, que nada tiene que ver el uso de estos sistemas con la simple videovigilancia u otros tratamientos de datos, por preocupantes que sigan siendo. Y lo mismo respecto de los sistemas biométricos de categorización, reconocimiento de emociones y evaluación de la personalidad, tanto o más peligrosos. Estos sistemas suponen contar a gran escala con la evaluación que puede realizar de una persona un excelente psicólogo y así leer emociones, detectar la verdad de las manifestaciones o expresiones de la persona o incluso predecir futuros comportamientos. Paradójicamente, estos sistemas de categorización, reconocimiento de emociones y evaluación de la personalidad cuentan con menor protección tanto en el RGPD[6] como -si no cambia- en el futuro Reglamento de IA de la UE (RIA).[7]

Con estas tecnologías, ahora en milisegundos se capta la imagen de una persona, se genera una plantilla y se compara, por ejemplo, con las plantillas de personas buscadas. O se pueden generar automatizadamente grandes cantidades de datos procesados que pueden ser utilizados para múltiples finalidades. Estos datos son especialmente utilizados con finalidades de seguridad pública. En España sólo se puede intuir que así sucede dada la total opacidad en la materia. Y es que cuando se ha ejercido el derecho de acceso a la información pública al respecto a autoridades policiales sobre el uso de

---

identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos", en Balaguer, Francisco y Cotino, Lorenzo, *Derecho público de la inteligencia artificial*, F. Jiménez Abad-Marcial Pons, 2023.

[6] Desde el Parlamento UE se afirma que "no parece normal que queden bajo el régimen general las emociones, los pensamientos y las intenciones". Parlamento Unión Europea (Wendehorst, Christiane y Duller, Yannic), *Biometric Recognition and Behavioural Detection*, Policy Department for Citizens' Rights and Constitutional Affairs , Directorate-General for Internal Policies, agosto 2021. El FRA ya señaló la especial sensibilidad de estos sistemas (FRA- Agencia de la Unión Europea para los Derechos Fundamentales, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, Luxembourg, Publications Office, 2020. Y no hay que olvidar que e CEPD y el SEPD quieren en general prohibirlos (ver nº 35), CEPD-SEPD, *Dictamen conjunto 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia artificial),*2021.

También se ha pedido que se prohíban totalmente las aplicaciones que permiten la "categorización biométrica", ver, EDRI (Montag L. y otros), *The Rise and rise of biometrics mass surveillance in the EU, A legal analysis of biometrics mass surveillance practices in Germany, the Netherlands, and Poland*, EDRi - European Digital Rights, 2021.

[7] Propuesta de Reglamento del Parlamento Europeo y del Consejo que se establecen normas armonizadas sobre la inteligencia artificial (Ley de Inteligencia Artificial). El último texto conocido es de la Presidencia Checa de 6 de diciembre 2022.

estos sistemas, las respuestas han sido por lo general muy insatisfactorias. Por lo general se alegan cuestiones de seguridad para no dar ninguna información (art. 14 Ley 19/2013). Es más, incluso se acude a que el uso de tecnologías policiales es desde 1985 materia clasificada[8]. Ello no sólo lleva a la opacidad, sino que además conlleva que estas tecnologías ni siquiera queden bajo el ámbito de aplicación de la Ley Orgánica 7/2021 (art. 2. 3º d). Es decir, ni siquiera sería aplicable la reciente ley que específicamente regula los tratamientos de datos en materia criminal y de seguridad. Nadie cuestiona que lo normal en el ámbito policial y criminal será la excepción de la transparencia y acceso a la información (Considerando 26 Directiva (UE) 2016/680). Es la ley nacional la que debe regular -y bien- estas excepciones de las obligaciones de informar. A este respecto, la FRA insiste en la necesaria justificación de las restricciones a la transparencia[9]. Y aunque se regulen y justifiquen restricciones en cualquier caso, el responsable del tratamiento deberá garantizar que se facilite efectivamente un mínimo de información[10]. Estos requisitos no se cumplen en España.

El reconocimiento facial, los sistemas automatizados y tecnologías conexas suponen disparar y con fuego racheado a los derechos fundamentales[11]. Inciden especialmente en las garantías del debido proceso o la no discriminación. Ello supone tener en cuenta muchas garantías ya exigibles a los sistemas IA. Y en todo caso, la protección de datos sigue siendo por defecto la regulación aplicable cuando estos sistemas traten datos personales. El régimen de protección de datos es bien sólido y ha permitido generar ya una destilada regulación y jurisprudencia europea y española claramente proyectable a

[8] Me remito a la investigación coordinada por el equipo liderado por Lucía Martínez Garay Universidad de Valencia-Amnistía Internacional sobre sistemas IA públicos del ámbito policial y penitenciario. En concreto, derechos de acceso ejercidos por uno de los miembros del equipo frente a la Guardia Civil (Exp. Transp. nº 062893) y los Mossos d'Esquadra (19 de noviembre de 2021, respuesta 18 de enero de 2022). En el caso de la Guardia Civil, se afirma que estos sistemas de identificación biométrica quedan afectados por Acuerdo del Consejo de Ministros de 28 de noviembre de 1986, ampliado por Acuerdos de 17 de marzo y 29 de julio de 1994, otorga el carácter de "Reservado" a aquella información relativa a "las plantillas de personal y medios y de equipo de las Unidades". En el caso de solicitud de información sobre Sistema Automático de Identificación Biométrica (ABIS) (nº expediente: 001-062892, la denegación es en razón del artículo 14 Ley 19/2013.

[9] FRA, *Facial recognition technology*… cit., p. 24.

[10] CEPD, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, Version 1.0, 12 mayo 2022, ver nº 85, 22-23 y nº 87. Asimismo, cabe seguir especialmente el artículo 13.2º Directiva (UE) 2016/680.

[11] Entre otros, los diversos estudios en Cotino Hueso, Lorenzo (editor), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Thompson-Reuters Aranzadi, Cizur, 2022, una visión general en Presno Linera, Miguel Ángel, *Derechos fundamentales e inteligencia artificial*, Marcial Pons, Madrid, 2023.

estos sistemas[12]. Y como muestra, un botón: frente el fuerte impacto social que desde fines de 2022 ha supuesto *Chatgpt*, ya ha habido respuesta sobre la base de la protección de datos, como la prohibición de este sistema en Italia por el *Garante* de la protección de datos en marzo y abril 2023[13]. Y el Comité Europeo de Protección de datos (CEPD) ha sido consultado por la AEPD al respecto[14]. Hoy por hoy el régimen de protección de datos es la principal respuesta regulatoria frente a los sistemas IA. Hasta el futuro RIA, sobre el que volveremos en las conclusiones.

Pues bien, como a continuación se analiza, el nivel de exigencias constitucionales a la regulación legal del uso de sistemas automatizados es extraordinariamente alta por el TC alemán. Ello es así esencialmente a partir del derecho de protección de datos. A partir del análisis, se reflexionará y concluirá que, pese a la acción regulatoria especialmente desde la UE, el legislador español no está asumiendo las responsabilidades que le corresponden. Ello no sólo va en perjuicio de los derechos fundamentales de la ciudadanía, sino que también posterga a la oscuridad e inseguridad jurídica a los positivos usos de estas tecnologías.

II. LOS PRESUPUESTOS DE LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL ALEMÁN DE 2023, QUE DECLARA LA NULIDAD DE LA EVALUACIÓN O ANÁLISIS AUTOMATIZADO DE DATOS CON FINES POLICIALES

1. La Sentencia y la regulación analizada

La Sentencia de 16 de febrero de 2023 (1 BvR 1547/19, 1 BvR 2634/20) de la primera cámara del Tribunal Constitucional Federal (TCF)[15] es una sentencia amplia, de unas 30 mil palabras con 178 párrafos. Esta sentencia resuelve los recursos de inconstitucionalidad presentados en 2019, frente a dos leyes prácticamente idénticas: el parágrafo § 25a párrafo 1 1º de la ley de Hesse sobre seguridad y orden público (*HSOG*), versión del 25 de junio de 2018[16]. Y la Sección 49 de la Ley de Procesamiento

[12] Entre otros, cabe seguir AEPD, *Adecuación al RGPD de tratamientos que incorporan Inteligencia artificial. Una introducción*, 2020, ; AEPD, *Requisitos para Auditorías de Tratamientos que incluyan Inteligencia artificial*, 2021.

[13] Provvedimento del 30 marzo 2023 [9870832] y de 11 de abril 2023 [9874702]. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870832

[14] "Spain asks EU data protection board to discuss OpenAI's ChatGPT", Reuters, 11.4.2023.

[15] https://www.bundesverfassungsgericht.de/e/rs20230216_1bvr154719.html. resulta de interés también el comunicado de prensa n° 18/2023 de 16 de febrero de 2023 en inglés y alemán. Las referencias a la misma en español son a partir de traducción automatizada.

[16] "§ 25a HSOG - Aplicación automatizada para análisis de datos. (1) En casos individuales justificados, las autoridades policiales pueden procesar adicionalmente los datos personales almacenados utilizando una aplicación automatizada para el análisis de datos para combatir

de Datos de la Policía de Hamburgo (*PolDVG*) en versión de 12 de diciembre de 2019[17]. Además de los gobiernos de estos Estados, participaron el Comisionado de Protección de Datos y Libertad de Información de Hesse, la Autoridad de Justicia y Protección del Consumidor Hamburgo y el Comisionado de Hamburgo de Protección de Datos y Libertad de Información. También emitió declaraciones el Comisionado Federal de Protección de Datos y Libertad de Información.

Estas leyes, como más tarde se detalla (& 120 y ss.), permiten y utilizar bases de datos y vincularlas a una aplicación automatizada, una plataforma para el "análisis" de datos (Hesse) o una "evaluación" de datos (Hamburgo) por la policía para evitar peligros[18]. A partir de dicho procesamiento de datos "se pueden crear relaciones o conexiones entre personas, grupos de personas, instituciones, organizaciones, objetos y cosas, se pueden excluir información y hallazgos insignificantes, los hallazgos entrantes se pueden asignar a los hechos conocidos y los datos almacenados pueden evaluarse estadísticamente."(§ 25a 2º HSOG). Todo ello, para combatir determinados delitos, o

---

preventivamente los delitos a los que se refiere el artículo 100a (2) del Código de Procedimiento Penal o para evitar una amenaza para la existencia o seguridad de la Federación o una Tierra o Vida, miembro o libertad de una persona o propiedad de valor significativo, cuya preservación es de interés público, o si se espera un daño equivalente al medio ambiente.

(2) Como parte del procesamiento posterior de acuerdo con el párrafo 1, se pueden crear relaciones o conexiones entre personas, grupos de personas, instituciones, organizaciones, objetos y cosas, se pueden excluir información y hallazgos insignificantes, los hallazgos entrantes se pueden asignar a los hechos conocidos y los datos almacenados pueden evaluarse estadísticamente.

(3) 1. El establecimiento y los cambios significativos en una aplicación automatizada para el análisis de datos se llevan a cabo por orden de la administración de la autoridad o de un empleado comisionado por ella. 2 Se debe consultar al oficial de protección de datos de Hessian antes del establecimiento o cambio significativo de conformidad con la oración 1; en caso de peligro inminente, la audiencia deberá celebrarse en una fecha posterior." (traducción automatizada).

[17] "§ 49 Aplicación automatizada para la evaluación de datos existentes. (1) En casos individuales justificados, la policía podrá procesar datos personales almacenados en los sistemas de ficheros policiales mediante una aplicación automatizada para la evaluación de datos, si ello es necesario para la lucha preventiva contra los delitos penales a que se refiere el apartado 2 del artículo 100a de la Ley de Enjuiciamiento Criminal o para la prevención de un peligro para la existencia o la seguridad de la Federación o de un Estado federado o para la vida, la integridad física o la libertad de una persona o de bienes de valor significativo, cuya conservación sea necesaria en interés público.

(2) En el marco del tratamiento conforme al apartado 1, podrán establecerse, en particular, relaciones o conexiones entre personas, grupos de personas, instituciones, organizaciones, objetos y cosas, podrán excluirse informaciones y constataciones insignificantes, podrán asignarse las constataciones entrantes a hechos conocidos y podrán evaluarse estadísticamente los datos almacenados.

(3) El establecimiento y la modificación sustancial de una aplicación automatizada conforme al apartado 1 se efectuarán por orden del Jefe de Policía o de la representación de turno. El Comisario de Protección de Datos y Libertad de Información de Hamburgo será oído antes del establecimiento o de la modificación sustancial conforme a la frase 1; en caso de peligro inminente, la audiencia se celebrará con posterioridad." (traducción automatizada).

[18] La sentencia trata de modo indiferenciado una u otra expresión (&149).

evitar amenazas y daños relevantes y de interés público. Esta regulación legal se remite a la configuración concreta del sistema automatizado por orden de la administración de la autoridad o de un empleado comisionado por ella con una consulta previa al delegado de protección de datos.

En Hesse, la plataforma "*hessenDATA*" se utilizó alrededor de 14 000 casos por año, de los cuales 2000 para evitar peligros (25a 1º. 2º HSOG) y en 12 000 casos para prevención (25a 1º. 1º HSOG). En Hamburgo no puso en práctica.

La sentencia insiste en el plus e intensidad que implica el análisis o interpretación *automatizada* de los datos: "el análisis o evaluación de datos automatizados tiene potencialmente su propio peso" (&54), esto es, el conocimiento que se puede obtener. Se trata de una restricción cualificada, que va más allá de que los datos personales se utilicen para otra finalidad que para la que se recabaron.

Pues bien, el párrafo primero de estas leyes se considera nulo por el TCF (&1 y 2, & 173) por violar el libre desarrollo de la personalidad del artículo 2. 1º[19] en conjunto con el artículo 1 (dignidad de la persona)[20] de la Ley fundamental. Desde los & 55 y ss. se realiza el análisis por el TCF, inicialmente sobre la posibilidad y requisitos constitucionales para el cambio de finalidad de uso de datos; y después (&66 y ss.) sobre los requisitos constitucionales de la intervención, autorización legal, intensidad y garantías añadidas. Más adelante, el TC especifica las muchas garantías que debería incorporar la regulación legal según la intensidad de la intervención (& 103 y ss.). Todo ello para concluir los elevados estándares que la sentencia afirma no los cumplen las leyes impugnadas, lo cual conlleva su inconstitucionalidad (&123 y ss.)

Así, se concluye esencialmente que la regulación legal cuestionada tiene una redacción particularmente amplia de los poderes para la realización de tratamientos de datos automatizados, sin que en modo alguno se regule de modo suficiente el peligro identificable que puede permitir estos tratamientos de datos, ni los datos concretos a tratar y los métodos a utilizar. Estas carencias legales suponen no alcanzar los requisitos constitucionales para el umbral o intensidad de la intrusión legal e interferencia en los derechos fundamentales.

2. Como punto de partida general, sí es legítimo y necesario hacer tratamientos automatizados de datos para la prevención de delitos

[19] "La dignidad humana es intangible. Respetarla y protegerla es obligación de todo poder público."

[20] "Toda persona tiene el derecho al libre desarrollo de su personalidad siempre que no viole los derechos de otros ni atente contra el orden constitucional o la ley moral."

Con carácter general se afirma la finalidad legítima y necesidad de tratamientos automatizados de datos: el "propósito legítimo de aumentar la eficacia de la prevención de actos delictivos grave en el contexto de la evolución de las tecnologías de la información mediante la obtención de indicios de delitos graves inminentes que, de otro modo, pasarían desapercibidos en la base de datos de la policía. […] las autoridades policiales se enfrentan a un volumen de datos en constante crecimiento y cada vez más heterogéneo en términos de su calidad y formato [y el conocimiento…] difícilmente podría obtenerse manualmente, especialmente bajo presión de tiempo" &52. Se recuerda que el uso de sistemas automatizados solo está permitido para proteger intereses legales particularmente importantes, como la vida, la integridad física o la libertad de la persona. Se requiere un peligro suficientemente identificable (*hinreichend konkretisierte Gefahr*, &58). No obstante y como se verá, se precisa concretar bastante el presupuesto de uso de estos sistemas automatizados para su admisibilidad específica.

Por cuanto al uso de datos para otra finalidad que por la que inicialmente fueron recabados (& 55 y ss.), en principio, "El uso posterior dentro del propósito original solo puede ser considerado por la misma autoridad dentro del alcance de la misma tarea y para la protección de los mismos intereses legales que para la recopilación de datos" (&57). Usarlos para otra finalidad es una nueva restricción de la protección de datos más allá de la recopilación inicial (&60), se necesita una finalidad "suficientemente específica" (&62), más allá de la investigación específica que motivó inicialmente la medida de recopilación para otros fines, "cada nuevo uso de los datos debe estar justificado por un peligro urgente o suficientemente específico en el caso individual" (&64).

3. La variable intensidad del rastreo, métodos y técnicas y datos utilizados y, en consecuencia, de la respuesta y garantías de la regulación legal

De manera muy minuciosa el TCF detalla los diversos criterios para determinar la mayor o menor intensidad de la injerencia (&76 y ss.). En general, se apuntan factores como: la mayor o menor duración del rastreo, si incluyen datos de rastreo espaciales o geográficos, si derivan perfilados de la personalidad, si se obtiene información que sirva como punto de partida para otras medidas no relacionadas con lo que motivó la intervención inicial, si hay tecnología de reconocimiento automatizado, si hay riesgos específicos de discriminación (&78).

Respecto de los factores variables según la "naturaleza y alcance de los datos" que se tratan (&78 y ss.) se apuntan también diversos criterios: la cantidad de datos, los diversos tipos de datos utilizados conjuntamente, la relevancia inherente de los datos, el origen de los mismos o si hay datos de redes sociales. Los requisitos son más estrictos

en el caso de datos obtenidos a través de la vigilancia de domicilios particulares o registros remotos de sistemas informáticos. (&81).

El TC alemán apunta la importancia de los métodos de análisis de datos para afectar a la personalidad de los interesados, “pueden surgir nuevas formas respaldadas por software de completar la imagen de una persona si se incluyen datos y suposiciones calculadas algorítmicamente sobre las relaciones y los contextos del entorno de las personas afectadas. […] adquiere así un impacto mucho mayor (cf. *BVerfGE* 115, 320 <356 f.> mwN -) si se incluyen datos y suposiciones calculadas algorítmicamente sobre las relaciones y conexiones del entorno de los afectados.” (&69) “[L]a aplicación automatizada puede cambiar decisivamente la forma en que trabaja la policía y cómo puede obtener información y, por lo tanto, también puede aumentar significativamente el peso del menoscabo individual” (&70). La variable intensidad de la restricción se hace depender de los “métodos de análisis o evaluación” (&90 y ss.): “en general, el método de análisis o evaluación de datos automatizados es tanto más intensivo en intervención, cuanto más amplio y profundo se puede obtener un conocimiento sobre las personas, mayor es la susceptibilidad al error y la discriminación, y más difícil es entender el software.” (&90). Los tipos de búsquedas que permite la plataforma o sistema son relevantes para la intensidad de la restricción. Así, hay mayor peligro si el sistema permite “no en un término de búsqueda relacionado con los hechos previamente reconocibles”. Cuantos menos requisitos de búsqueda de datos exija el legislador, más peligro.

Asimismo, “La intervención se intensifica en particular si, en el sentido de "vigilancia predictiva", las máquinas hacen afirmaciones peligrosas sobre personas” (&98). La “inteligencia artificial (IA), puede tener un peso particular en la intervención”, un “valor añadido” con “peligros específicos [por] que no sólo los patrones criminológicamente bien fundados son utilizados por los agentes de policía individuales, sino que dichos patrones se desarrollan automáticamente […] los sistemas algorítmicos complejos podrían separarse cada vez más de la programación humana original en el curso del proceso de aprendizaje automático”. Además, “Si se utiliza software de actores privados u otros estados, también existe el riesgo de manipulación inadvertida o acceso inadvertido a los datos por parte de terceros” (&100).

Pues bien, a partir de las variables intervenciones en los derechos, los requisitos constitucionales para el legislador son también variables (&103 y ss.): “El que una autorización para el análisis o evaluación de datos automatizados satisfaga los requisitos constitucionales también depende de si el legislador ha regulado las condiciones suficientes para la intervención en vista de la forma específica de la autorización […]el legislador dispone de un amplio abanico de opciones para controlar el peso de la

intervención en la autodeterminación informativa asociada al análisis o evaluación de datos automatizados de forma que sea proporcional al respectivo umbral de intervención y sobre el peso de la prevención de riesgos pretendida" (&103).

III. LOS ELEVADOS ESTÁNDARES DE CALIDAD DE LA LEY QUE FIJA EL TRIBUNAL CONSTITUCIONAL ALEMÁN

1. Cómo regular con garantías los presupuestos de uso de sistemas automatizados de análisis de datos

Por cuanto a la finalidad o interés jurídico que legitima la restricción de derechos, son diversas las técnicas regulatorias que menciona el TCF y de las que procede tomar buena nota:

> "El legislador también puede abstenerse de nombrar directamente el interés jurídico exigido y en su lugar vincularlo a las infracciones penales correspondientes, cuya prevención se pretende" (&106).

Sobre los indicios sobre la existencia de un peligro concreto, "Los enunciados empíricos generales por sí solos no son suficientes a este respecto […] los hechos deben permitir concluir que el evento es al menos de un tipo específico y previsible en el tiempo, y por otro lado que estarán involucradas ciertas personas cuya identidad se conoce al menos lo suficiente para la medida de vigilancia. para ser utilizado específicamente contra ellos y en gran medida puede limitarse a ellos." (&106).

"Las intervenciones menos serias pueden justificarse por razones menores […] En algunos casos, el cumplimiento del principio de limitación de la finalidad puede incluso ser suficiente (& 107).

Más tarde, el TCF (&152 ss.) se muestra especialmente riguroso por cuanto el legislador tampoco ha determinado estrictamente los motivos o presupuestos bajo los que se pueden realizar estos tratamientos automatizados de datos. En ningún caso se da el peligro concreto requerido: "el fin de prevenir la delitos penales […], el motivo de la intervención es desproporcionadamente amplio en vista de la gravedad de la intervención descrita" (&153); "no se especifica suficientemente el motivo de la intervención y no se cumple el requisito de al menos un riesgo especificado". En el caso de Hesse se habla de delito "esperado", lo cual tampoco es suficiente.

Aunque reconoce que es buen camino, tampoco es bastante que la ley afirme "que debe existir un "caso individual" justificado" (&155); para el TCF se necesitan especificaciones más detalladas. No estima suficiente que en la vista oral se hablara de utilizar el sistema automatizado respecto "un delito ya cometido o al menos a la

sospecha fácticamente probada de un delito ya cometido". (&159) Ello no limitaría suficientemente las facultades de análisis de datos por cuanto "a partir de una suposición abstracta de que ciertos delitos se cometen en serie, se llega a la conclusión general de que existe el riesgo de que se cometan esos delitos en el futuro" (&161). También el TCF señala que sería necesario que "se examin[e] también más de cerca si los datos individuales incluidos en el análisis son adecuados para contribuir a la prevención del delito en serie que puede ser inminente." No obstante, se considera que ello obligaría a incluir otras bases de datos y sería también desproporcionado (&162). La afirmación de que en el caso de Hesse esté "previsto un examen caso por caso de la idoneidad de los datos disponibles" tampoco parece ser suficiente (&163).

Sin embargo, el TCF da cierta luz de cómo podría regularse con garantías suficientes el presupuesto del uso de estas plataformas y aplicaciones: "Si, por el contrario, el poder fuera más limitado en términos del tipo y alcance de los datos y métodos de procesamiento permitidos y la intensidad potencial de la interferencia se redujera hasta tal punto que un umbral de interferencia más bajo sería constitucionalmente suficiente […] el concepto actual de la práctica de Hesse podría ser el punto de partida para un diseño constitucionalmente compatible de los requisitos de intervención […] tal concepto tendría entonces que ser regulado más detalladamente cumpliendo con los requisitos de la reserva estatutaria, la claridad de las normas y el requisito de certeza." (&165).

Así, con miras a futuras regulaciones, se apunta que la utilización de sistemas de análisis de datos en supuestos individuales y específicos sí que pueda ser suficiente: "la autorización presupone que una medida debe ser necesaria en un caso individual para evitar un peligro, ésta puede reemplazar una especificación más detallada del requisito de peligro y considerarse una descripción suficientemente específica del requisito de un peligro concreto […] si la medida en sí misma no invade profundamente la esfera privada" (&166). Se recuerda en todo caso la sentencia de 26 de abril de 2022 - 1 BvR 1619/17 -, párr. 206[21] respecto de la legislación antiterrorista federal, una regulación más garantista y restrictiva que las de Hesse y Hamburgo. En aquel caso se afirmó que: "sería inadmisible una medida que se llevara a cabo en la oscuridad, sin nombrar y justificar sobre la base de qué indicios fácticos se adopta y cómo se pretende contribuir a la investigación. Si la medida se dirige específicamente contra determinadas personas, la vigilancia de éstas en particular debe contribuir al esclarecimiento de hechos. La urgencia de una medida puede disminuir cuanto más tiempo se utilice sin que produzca resultados significativos. La calidad de la información obtenida debe evaluarse continuamente (véase también el artículo 19, apartado 2, frase 5, de la BayVSG)."

[21] http://www.bverfg.de/e/rs20220426_1bvr161917.html

(&206). Estos elementos deben ser tenidos en cuenta a la hora de regular presupuestos de uso de estos sistemas automatizados.

Frente a estas exigencias, la sentencia ahora analizada se censura que la leyes de Hamburgo y Hesse permiten un uso prolongado y no específico del sistema (&167), además de que se permite el uso con la finalidad de adquirir conocimientos para futuras investigaciones y procedimientos de investigación, sin un peligro congreso o particular.

2. Los mínimos que la ley debe regular a la hora de concretar las técnicas y tratamientos automatizados posibles y los límites que tienen los reglamentos o las autoridades

El TCF permite la colaboración normativa y remisión legal a las autoridades (&110 y ss.). Así, “En principio, el legislador puede dividir esta tarea normativa entre él mismo y la administración (1). Sin embargo, debe asegurarse de que, cumpliendo con la disposición legal, se establezcan suficientes regulaciones, en particular para limitar el tipo y el alcance de los datos (2) y para limitar los métodos de procesamiento de datos (3).” (&110). Se afirma que “el legislador puede exigir a las autoridades administrativas que especifiquen con mayor precisión las determinaciones abstractas […] la especificación mediante normas administrativas requiere en todo caso una base legal […] el legislador debe asegurarse de que las autoridades documenten y publiquen de manera comprensible las determinaciones de precisión y uniformidad que regirán en última instancia la aplicación de las disposiciones en el caso particular […] puede exigir a las autoridades administrativas que especifiquen más las determinaciones abstractas y generales (&113).

En todo caso, pese a esta colaboración normativa y remisión a autoridades, el TCF sí que indica los mínimos que sí que ha de regular la ley y establece también la prohibición de sistemas de autoaprendizaje. Así:

- “la propia ley deberá regular qué bases de datos se pueden incluir y en qué medida se puede automatizar” (&116),

- “el legislador también debe asegurarse de limitar el uso automatizado al que solo tienen acceso los empleados policiales debidamente calificados […no obstante] Los detalles técnicos pueden ser regulados en reglamentos administrativos a ser publicados.” (&117)

- “la propia ley debe regular que los datos obtenidos de la vigilancia domiciliaria o búsquedas en línea se utilicen en un análisis o evaluación de datos que sirva para evitar que se cometan delitos (&118),

- el “uso posterior debe limitarse […] a partir de enfoques de investigación concretos […] de importancia comparable” (&118),

- “también debe regular […] precauciones técnicas y organizativas apropiadas” (&118),

- “la información procedente de la recopilación intensiva de datos debe marcarse o separarse con antelación para impedir el acceso en caso necesario y no debe identificarse posteriormente”. (&118),

- “respecto al tipo y alcance de los datos que se pueden utilizar en el análisis o evaluación de datos automatizados […] la reserva legal también se aplica a este respecto” (&119)

- “Si el legislador desea reducir la intensidad de la intervención del análisis o evaluación de datos […] también debe hacer especificaciones restrictivas para el método de los datos automatizados.” (&120)

Por cuanto a las posibilidades de configuración del sistema automatizado por las autoridades, el TCF expresamente obliga a que la ley limite las posibilidades e impone limitaciones a la automatización, e incluso prohibición de sistemas de autoaprendizaje: “El uso de sistemas de autoaprendizaje debe estar expresamente excluido en la ley. Además, el propio poder legislativo debe adoptar disposiciones básicas para limitar el grado de automatización […] habría que establecer en la propia ley una restricción a las opciones de comparación […] deben excluirse en particular las declaraciones de peligrosidad de las máquinas sobre personas en el sentido de "vigilancia predictiva", o el análisis o evaluación de los datos solo debe basarse en la detección de personas peligrosas o en peligro de extinción desde el principio […] el peso de la invasión solo se reduce si la propia legislatura así lo especifica.” (&121).

3. Además, deben regularse garantías técnicas y organizativas

A estas garantías de regulación legal de los presupuestos para poder hacer los tratamientos automatizados de datos, se añaden garantías técnicas y organizativas. Así, “en cualquier caso, el principio de proporcionalidad se traduce en exigencias de transparencia, tutela jurídica individual y control de supervisión (& 103):

“un diseño apropiado del control es de gran importancia. En vista del número posiblemente alto de medidas, esto se puede dividir entre delegados de protección de datos independientes y oficiales de acuerdo con un concepto de control graduado y también regulado como un procedimiento aleatorio. Para un control

efectivo, es esencial que se proporcionen razones formuladas de forma independiente sobre por qué ciertas bases de datos se analizan por medios automatizados para prevenir ciertos delitos penales. Si se utiliza software, lo que permite formas más complejas de comparación automatizada de datos, también se requieren precauciones para evitar errores que están específicamente asociados con esto, lo que también puede requerir regulaciones legales sobre el estado de seguimiento del desarrollo del software utilizado. [no obstante] Los requisitos específicos que deben imponerse a la protección de acompañamiento no son objeto de este procedimiento." (&109). Aunque esta cuestión no sea objeto del procedimiento, sin duda, la regulación legal de las garantías específicas resulta un elemento esencial para el TC español y el artículo 23.2º RGPD.

4. La aplicación de tan elevados estándares conlleva la inconstitucionalidad de las leyes impugnadas

Como se habrá apreciado, los estándares que impone el TCF al legislador son muy elevados. Y basta compararlos con las leyes enjuiciadas para que la declaración de inconstitucionalidad sea clara, como se produce en los apartados &123 y ss. Son numerosas las carencias que se detectan. La legislación enjuiciada permite el tratamiento automatizado de cantidades ilimitadas de datos, mediante métodos que tampoco son determinados por la ley, "permiten a la policía crear perfiles completos de personas, grupos y entornos con un solo clic y también someter a numerosas personas legalmente ajenas a medidas policiales adicionales" (&149). Personas no sospechosas como testigos pueden quedar sometidos a medidas policiales prácticamente sin restricciones sobre el tipo y la cantidad de datos que pueden utilizarse, sin diferenciar de sospechosos.

De igual modo, el "legislador no ha restringido qué métodos de análisis y evaluación están permitidos" (&146). No hay límites respecto de "formas más complejas de comparación de datos […] permiten la "minería de datos" […] hasta el uso de sistemas de autoaprendizaje […] también se permiten búsquedas abiertas." Asimismo se recuerda que de la búsqueda de "anomalías estadísticas" que permite la ley "se pueden extraer conclusiones adicionales". Y las normas legales "tampoco excluyen nada con respecto a los resultados de búsqueda que se pueden lograr". De hecho, se afirma que "el resultado de la búsqueda podría consistir en evaluaciones automáticas de hechos, hasta declaraciones sobre el peligro de las personas en el sentido de "vigilancia predictiva" […]

se podría generar nueva información relacionada con la personalidad" (&147)[22]. La regulación no se acompaña de reglas con respecto a su uso que podrían reducir la gravedad de la interferencia. En Hamburgo "el cambio de redacción de "análisis de datos" a "evaluación de datos" no se logró una aclaración constitucionalmente suficiente" (&148).

IV. ESTA SENTENCIA SE SUMA A UNA CLARA LÍNEA JURISPRUDENCIAL EXIGENTE EN EUROPA Y ESPAÑA

El Tribunal Constitucional alemán, el más influyente de Europa, esencialmente a partir del derecho de protección de datos, impone una detallada regulación legal y de calidad respecto del uso de sistemas automatizados. Su decisión es muy exigente y rigurosa -quizá incluso en exceso- al fijar estándares de garantías y calidad legislativa. Es más, lo hace para el ámbito de lo público y en concreto y no por primera vez para el ámbito de la seguridad pública, es decir, un terreno en el que podría pensarse que hay mayor deferencia y tolerancia respecto de las restricciones de derechos y donde son menores las exigencias de garantías y calidad legislativa. No en vano y como adelantó al inicio, los tratamientos de datos para la seguridad pública o la defensa en España en ocasiones parecen un sumidero para las garantías de los derechos.

Si miramos la regulación española a la luz de los estándares de regulación que ahí se exigen, podemos comprobar muy fácilmente no llega, si se me permite, ni a la *suela de los zapatos* de las exigencias de aquel tribunal.

En 2020 ya alerté de algo similar con motivo de la histórica sentencia de 5 de febrero de 2020 del Tribunal de Distrito de la Haya (C / 09/550982 / HA ZA 18-388), que declaró

[22] "(a) Las disposiciones impugnadas no excluyen formas más complejas de comparación de datos. Si el § 25a HSOG y el § 49 HmbPolDVG hablan de la aplicación automatizada para el análisis de datos o la evaluación de datos, es decir, no de comparación (automatizada), esto ya se diferencia de la comparación simple en términos del sistema legal (ver § 25 HSOG, § 48 Apartado 1 HmbPolDVG) de distancia. La Sección 25a HSOG y la Sección 49 HmbPolDVG, por otro lado, permiten la "minería de datos" (cf. BVerfGE 156, 11 <40 párr. 74>) hasta el uso de sistemas de autoaprendizaje (KI). En particular, también se permiten búsquedas abiertas (cf. párr. 93 y siguientes). El análisis o evaluación de datos puede tener como objetivo descubrir solo anomalías estadísticas en los volúmenes de datos, a partir de las cuales se pueden extraer conclusiones adicionales, posiblemente también con la ayuda de otras aplicaciones automatizadas. Las disposiciones tampoco excluyen nada con respecto a los resultados de búsqueda que se pueden lograr (cf. párr. 96 y ss.); de acuerdo con la redacción, el resultado de la búsqueda podría consistir en evaluaciones automáticas de hechos, hasta declaraciones sobre el peligro de las personas en el sentido de "vigilancia predictiva". Por lo tanto, se podría generar nueva información relacionada con la personalidad mediante análisis o evaluación de datos, a la que de otro modo no habría acceso (cf. Bäuerle, en: Möstl/Bäuerle, BeckOK Police and Order Law Hessen, 27ª edición, a partir del 1 de octubre , 2022, § 25a HSOG, párrafo 21). Esta gama potencial de nuevos conocimientos alcanzables tampoco está flanqueada por reglas para mitigar el impacto en su uso".

contrario al artículo 8 CEDH sistema *Systeem Risicoindicatie* (*SyRI*)[23]. Se traté de una muy relevante sentencia sobre el tratamiento masivo de datos de modo automatizado con finalidades de aplicación de la ley. Y en aquel caso subrayé que la regulación neerlandesa que se declaraba contraria a diversos derechos fundamentales era amplia y contaba con muchas garantías y a pesar de ello se había considerado nula. Es decir, se declaraba allí inconstitucional una normativa con garantías que no se alcanzan ni de lejos en España respecto de los tratamientos masivos de datos que se llevan a cabo por la AEAT, la TGSS, CNMC o inspección de trabajo, entre otras. Tras aquella sentencia, la reacción en Países Bajos está siendo un ejemplo para toda la UE por cuanto a las medidas preventivas exigibles para la transparencia y explicabilidad de los algoritmos públicos así como para la evitación de sesgos[24]. También ha habido importantes decisiones por el Consejo Constitucional en Francia[25], donde se cuenta con una regulación indudablemente superior a la española[26]. Igualmente cabe mencionar las

[23] Puede seguirse especialmente mi estudio "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", en Carles Ramió (coord.), *Repensando la administración digital y la innovación pública*, Instituto Nacional de Administración Pública (INAP), Madrid, 2021. https://links.uv.es/FUW2pz6

También, "'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* nº 4, mayo 2020.

[24] Son muchos los documentos desde instituciones de Países Bajos. Destaca su estudio de impacto, Ministry Of The Interior And Kingdom, *Impact Assessment. Fundamental rights and algorithms (IAMA)*, Países Bajos, marzo. 2022

Respecto de sesgos e igualdad, Ministerie Van Binnenlandse Zaken; Van Der Sloot, B. y otros (2021): *Non-discriminatie by design,* encargo para (Ministerio del Interior), Tweede Kamer (Cámara de representantes). También, Ministerie Van Justitie En Veiligheid (Ministerio de Justicia y Seguridad), Rijksoverheid (Gobierno central), *Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses* (*Pautas para la aplicación de algoritmos por parte de los gobiernos y educación pública sobre análisis de datos*), Directiva (Richtlijn), de 08-03-2021, https://acortar.link/6C226N

En el ámbito de transparencia, el Excel desarrollado por el Algemene Rekenkamer (Tribunal de Cuentas), *Digitaal Toetsingskader Algoritmes (Marco de evaluación digital de Algoritmos)*, Tribunal de Cuentas, 2020, Excel.

De particular interés los criterios generales afirmados en el documento Ministerie Van Justitie En Veiligheid (Ministerio de Justicia y Seguridad), Rijksoverheid (Gobierno central) (2021), *Richtlijnen voor het toepassen van algoritmen door overheden en publieksvoorlichting over data-analyses* (*Pautas para la aplicación de algoritmos por parte de los gobiernos y educación pública sobre análisis de datos*), Directiva (Richtlijn), de 08-03-2021s.

[25] Esencialmente destacan de Consejo Constitucional francés: la Decisión N ° 2018-765 DC, 12 de junio de 2018 sobre la Ley nº 2016-1321 de 2016; la Decisión 2019-796 DC de 27 de diciembre, sobre la Loi de finances para 2020 y la decisión n° 2020-834 QPC del 3 de abril de 2020 sobre el sistema *Parcoursup* en el ámbito educativo.

[26] Esencialmente hay que tener en cuenta la LOI n° 2016-1321 du 7 octobre 2016 pour une République Numérique. JORF n° 0235 du 8 octobre 2016 y el desarrollo reglamentario, Decreto Nº 2017-330, de 14 de marzo de 2017, relativo a los derechos de las personas que sean objeto de

exigencias de regulación de calidad por el TC de Eslovaquia en su decisión de 17 de diciembre de 2021[27].

Y en modo alguno podemos pensar que nuestro TC español no es igual de exigente en materia de calidad legislativa de derechos fundamentales. De hecho la mejor doctrina jurisprudencial la ha desarrollado el TC con relación a la protección de datos. Así, inicialmente las SSTC 290/2000 (en especial, FJ 15º) y en la STC 17/2013 (y su voto particular). Pero sobre todo hay que tener en cuenta la STC 76/2019, de 22 de mayo (en especial FJ 8º). Se trata de una sentencia también muy rigurosa respecto de la necesidad de que la ley limitativa del derecho de protección de datos integre en su contenido no sólo el detalle de la restricción y sus presupuestos, sino que también se han de regular las garantías concretas compensatorias de la restricción.

Tampoco se puede decir que nuestras autoridades de protección de datos no sean sensibles a estos temas. Sin ir más lejos, el 20 de enero 2023 la AEPD ha vuelto a poner de manifiesto la falta de regulación legal suficiente respecto de sistemas biométricos[28]. Ello se suma al Informe 10308/2019 AEPD que no admitió el uso de sistemas de reconocimiento facial por servicios de seguridad privada. O las resoluciones de 2020 en las que la AEPD rechazó el uso reconocimiento facial con tecnologías avanzadas para evitar el fraude en exámenes por universidades online (e-proctoring, Informe 0036/2020, AEPD; resolución de advertencia E/05454/2021 AEPD), así como la Autoritat Catalana en 2023 (procedimiento PS 41/2022). Así como el más conocido caso *Mercadona* (procedimiento sancionador PS 120/2022 AEPD). El CEPD[29] ha sido bien claro también en 2022 respecto de las muchas garantías que deben darse en estos contextos. También es exhaustiva la FRA- Agencia de la Unión Europea para los Derechos Fundamentales[30] o desde el Parlamento Unión Europea[31] o el Consejo de Europa[32].

---

decisiones individuales adoptadas sobre el fundamento de un tratamiento algorítmico. Además de la normativa tributaria y en otros ámbitos específicos.

[27] Con relación a la normativa fiscal respecto de la recopilación masiva de datos de recibos y elaboración de perfiles de riesgo de las empresas, acceso completo en https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2021/492/20211217

[28] Dictamen 98/2022 de 20 de enero de 2023, en el que se declara la inconformidad con la normativa vigente reguladora de protección de datos de la adopción del acuerdo de la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia, en el ámbito de sus competencias dentro de la Liga Nacional de Fútbol Profesional, por el que se establecen medidas a tomar por parte de los clubes de futbol, en la instalación de sistemas biométricos para el control de todos los accesos a las gradas de animación que permita la identificación unívoca de los aficionados que accedan a dichas gradas.

[29] CEPD, *Guidelines 05/2022 … cit.*

[30] FRA, *Facial recognition technology… cit.*

[31] Parlamento Unión Europea (2020). *Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights*, Policy Department for Citizens' Rights and Constitutional Affairs , Directorate-

Tanto el Derecho Europeo como el Derecho Constitucional español son cada vez más exigentes con el principio de calidad normativa de los derechos fundamentales. Y precisamente los hitos se han dado en el ámbito de la protección de datos. Cabe destacar en general la STJUE (Gran Sala) de 8 de abril de 2014, Digital Rights Asuntos C-293/12 y C-594/12 (nº 54). La legislación debe establecer normas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e imponer salvaguardias para que las personas cuyos datos han sido tratados tengan garantías suficientes para proteger eficazmente sus datos personales contra el riesgo de abuso y contra cualquier acceso o uso ilícitos de esos datos[33]. La ley ha de establecer condiciones sustantivas y de procedimiento y criterios objetivos para determinar los límites del acceso de las autoridades competentes a los datos y su uso posterior.[34]

Y posiblemente no falte mucho para lo que puede ser una sentencia histórica para la UE en materia de decisiones automatizadas. El 26 de enero de 2023 ya se ha celebrado la audiencia oral pública en el caso C-634/21[35], el primero en el que se le ha pedido al TJUE que interprete el artículo 22 RGPD sobre decisiones automatizadas.

En Europa ya son *varias barbas de vecinos que han pelado*, sin embargo, *no parece que estemos remojando nuestra barba* con una legislación suficiente para el uso público de sistemas automatizados, en su caso de IA que impliquen un tratamiento masivo de datos.

V. PARA CONCLUIR: LA IMPERIOSA NECESIDAD DE REGULACIÓN DE CALIDAD EN ESPAÑA, INCLUSO CON EL FUTURO REGLAMENTO DE LA UNIÓN EUROPEA

Pese a la variada y concurrente normativa europea, sigue quedando un ámbito muy importante al legislador estatal. La ley (especialmente la nacional) ha de actuar para legitimar y garantizar de forma concreta cada sistema que implique un tratamiento de datos masivo y automatizado. Sin embargo, el legislador no está cumpliendo sus obligaciones. En el ámbito criminal y policial la Ley Orgánica 7/2021, de 26 de mayo no ha aportado prácticamente nada. En mayo de 2022, el CEPD ha recordado si la ley

---

General for Internal Policies julio. Ya citados, *Regulating facial recognition in the EU … cit. y Biometric Recognition and Behavioural Detection … cit.*

[32] Consejo de Europa, *Guidelines on Artificial intelligence and data protection*, 2019; Consejo de Europa, *Guidelines on Facial Recognition*, 2021,

[33] También STEDH de 1 de julio 2008, Liberty and Others v. the United Kingdom, 1 July 2008, nº 62 y 63. También Rotaru v. Rumanía, § 57 a 59, y S. y Marper contra el Reino Unido, § 99.

[34] De especial interés CEPD, 2022: nº 53 y 55, 15 y 16. Parlamento UE 2021 a): 35-42.

[35] Petición de decisión prejudicial planteada por el Verwaltungsgericht Wiesbaden (Alemania) el 15 de octubre de 2021 - OQ/Land Hesse.

nacional es una mera reiteración del artículo 10 Directiva 2016/680, no puede ser invocada como una ley que autoriza el tratamiento de datos biométricos[36].

Considero que en general no contamos con una ley habilitante y que regule las garantías respecto de un sistema de identificación biométrico concreto, ni para el sector público ni para el sector privado[37]. Y también en general, esto mismo se puede decir respecto de sistemas automatizados que permiten el tratamiento masivo de datos, más si cabe si son sistemas autónomos o con IA. Hoy día abundan las exclusiones de aplicación de normas por motivos de defensa y seguridad nacional o, como se expuso al inicio, se considera que los sistemas automatizados quedan bajo el régimen de materias clasificadas y, por esta vía se excluirían también de la aplicación de algunas normas, algo muy discutible. En todo caso, es obvio que estas exclusiones legales no excluyen de ningún modo la aplicación de la Constitución y los derechos fundamentales debido a su eficacia directa (art. 53 CE). Ello lo recuerda, por ejemplo, la sentencia del TC alemán de 19 de mayo de 2020 (1 *BvR* 2835/17)[38] que impone fuertes condiciones para la vigilancia de telecomunicaciones y tratamientos masivos de datos fuera de Alemania.

Esta insuficiencia de regulación legal en España no sólo se da respecto de tratamientos automatizados e IA en el ámbito penal y judicial. Se da también, por ejemplo, respecto de los tratamientos automatizados del ámbito tributario, tan preocupantes[39]. De hecho, la carencia legal es generalizada respecto del sector público ante la palmaria insuficiencia del artículo 41 Ley 40/2015 y sus escasos desarrollos. Esperemos que el apartado XVIII de la Carta de Derechos digitales sea un estímulo a la mejora regulatoria, como ha empezado a serlo con la Ley 15/2022, de 12 de julio de igualdad[40].

Ahora bien, esta insuficiencia de regulación legal y con garantías en España no preocupa en exceso. Y no sólo debería preocupar a quienes estudiamos y defendemos los derechos fundamentales de la ciudadanía. La falta de un legislador que cumpla con

---

[36] CEPD, *Guidelines 05/2022… cit.* , nº 71.

[37] Para este ámbito entiendo que la regulación de la videovigilancia *simple* tampoco sirve para legitimar las nuevas tecnologías biométricas, a partir del Informe 31/2019 AEPD para el ámbito de la seguridad privada. Para el ámbito de reconocimiento biométrico, algunos autores sí que consideran una suficiente base legal. Así, Izquierdo Carrasco, Manuel, "La utilización policial de los sistemas de reconocimiento facial automático. Comentario a la sentencia del Alto Tribunal de Justicia de Inglaterra y Gales de 4 de septiembre de 2019". *Revista Ius et Veritas,* núm. 60, mayo (2020), pp. 86-103, p. 71.

[38] https://www.bundesverfassungsgericht.de/e/rs20200519_1bvr283517.html

[39] Olivares Olivares, Bernardo D., "Law and Artificial Intelligence in the Spanish Tax Administration: the Need for a Specific Regulation", *European Review of Digital Administration* & Law-ERDAL 1 (1-2), p. 227-234.

[40] Puede seguirse mi estudio, "Derechos ante la administración digital y la inteligencia artificial (XVIII Y XV)", en Cotino Hueso, Lorenzo (editor), *La Carta de Derechos Digitales*, Tirant Lo Blanch, Valencia, 2022, pp. 251-284.

sus *deberes*, además, está privando del uso (legítimo) de estas tecnologías en ámbitos de seguridad en las que podrían ser muy útiles, así como en otros ámbitos públicos y privados: fraude, salud, educación, laboral, personalización de servicios públicos, marketing y un largo etcétera. Y lo que es peor, la inseguridad jurídica conlleva la ineficacia real de estos sistemas, por cuanto su utilización podría acarrear la nulidad de actuaciones públicas en estos contextos por vulneración de derechos fundamentales.

Considero que es muy buena ocasión para regular mejor y tomar al menos como modelo las *lecciones* que claramente se pueden extraer de la sentencia alemana. Pese a que puedan considerarse muy rigurosos estos criterios, pueden tomarse como punto de partida para hacer propuestas regulatorias. Ahora bien, creo que no debe orillarse o directamente prohibirse la regulación del uso de IA y los sistemas autónomos como hace sin excesiva justificación el TC alemán. De hecho, la futura regulación del RIA puede ser un impulso para la aceptación de estas tecnologías en ámbitos de aplicación de la ley, eso sí, con los estándares y garantías necesarios que implica el Reglamento y, sobre todo, con su compatibilización con la normativa de protección de datos y otros derechos fundamentales.

Pronto, a la normativa de protección de datos y otras aplicables se sumará el nuevo RIA. Este reglamento implicará muchas obligaciones y garantías para los llamados sistemas de “alto riesgo”, que habrán de cumplir el RIA[41] y, con él, las normas armonizadas que lo acompañarán. En el ámbito afín al de la sentencia alemana, cabe señalar que el RIA tendrá especial incidencia respecto de los sistemas de identificación biométrica. También se consideran de alto riesgo muchos usos públicos de IA en el ámbito de seguridad y aplicación de la ley. Así las cosas, se dará una importante y compleja concurrencia y superposición de regímenes jurídicos, especialmente de protección de datos y el RIA.

En algunos casos, el RIA impone especiales requisitos y garantías a la regulación legal de sistemas de identificación biométrica para que no se consideren prohibidos (art. 5 RIA, Anexo III). Se trata de garantías de regulación legal y de calidad a superponer con las ya exigibles por protección de datos u otros motivos.

Ahora bien, no está del todo claro si el propio RIA, con sus muchas garantías, puede valer para cumplir con las exigencias de regulación legal y de calidad que hoy por hoy se exigen constitucionalmente y en razón de la propia normativa de protección de datos.

[41] Una visión general del RIA en Hernández Peña, Juan Carlos, *El marco jurídico de la inteligencia artificial. Principios, procedimientos y estructuras de gobernanza*, Aranzadi, Cízur, 2022. Para el ámbito de la identificación biométrica en particular Cotino Hueso, Lorenzo, "Sistemas de inteligencia artificial con reconocimiento facial… cit.

Para instituciones como el CEPD-SEPD[42] o el Parlamento UE[43], en el ámbito de la identificación biométrica con IA, el RIA no sirve como la regulación legal que se exige en razón de la normativa de protección de datos, sino que se precisa una regulación legal específica y de calidad que habilite los tratamientos y regule garantías concretas. Quién suscribe también lo considera.

En todo caso, no puede ignorarse que el futuro RIA conlleva toda una auténtica batería de garantías, medidas técnicas y organizativas y de transparencia antes, durante y después del desarrollo de estos sistemas IA y su uso. Así las cosas, el reglamento europeo sí puede servir para descargar la necesidad de que una regulación legal específica establezca garantías. Es bien posible que la regulación legal concreta pueda, sobre la base del reglamento, fijar o modular las particulares garantías que deban aplicarse. En cualquier caso, no es una cuestión clara ni está bien regulada, por lo que el RIA debería aclararla en lo posible[44] para evitar incertidumbres que solo se resuelvan jurisprudencialmente con años de retraso.

Para la STC 76/2019, de 22 de mayo, las garantías propias y generales que regula el RGPD y la propia Ley orgánica 3/2018 de protección de datos no fueron suficientes, sino que se precisaba una regulación legal específica con garantías, lo que derivó en la inconstitucionalidad. En esta línea, considero que con la entrada en vigor del RIA, en general deben seguir exigiéndose las garantías y estándares de calidad legislativa tan seriamente fijados por el tribunal alemán para tratamientos automatizados, puesto que no se trataba de sistemas autónomos. En todo caso, el RIA se integrará en un conjunto normativo de nivel legal que tendrá que dar seguridad, certeza y garantías legales suficientes respecto del uso de estos sistemas.

[42] CEPD-SEPD, *Dictamen conjunto 5/2021… cit.* nº 31.

[43] Parlamento Unión Europea, *Regulating facial recognition* … cit.

[44] En el texto del AIA esto solamente puede deducirse del Considerando 24 propuesta del AIA y puede quedar sujeto a interpretaciones.