



VNIVERSIDAD
D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

INFORME

**LAYERED VOICE ANÁLISIS. HERRAMIENTA DE EVALUACIÓN Y
DETERMINACIÓN DE RIESGOS: PRECALIFICACIÓN DE EMPLEO,
SEGUIMIENTO Y CUESTIONARIOS A LA MEDIDA**

Elaborado por:

D. Daniel Terrón Santos

Profesor Titular de Derecho Administrativo

Universidad de Salamanca



UNIVERSIDAD
DE SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

ÍNDICE

I. *Layered Voice Analysis*. Inteligencia artificial predictiva

II. Regulación y límites

- a. Reglamento europeo sobre el uso de Inteligencia Artificial
- b. Plan nacional de Desarrollo de la IA en China
- c. Estados Unidos
- d. Arabia Saudí
- e. México
- f. Brasil
- g. Irak

III. Consideraciones legales sobre el análisis de datos biométricos.

Jurisprudencia y resoluciones al respecto

a. Resoluciones de la Agencia Española de Protección de Datos

- i. Mobile World Congress – Expediente 202100603,
- ii. Consejería de Sanidad de Castilla la Mancha - Expediente N.º: PS/00441/2021¹
- iii. Mercadona. Procedimiento sancionador N°PS/00120/2021 sobre reconocimiento facial.
- iv. Consulta N/REF: 0098/2022

b. Otras resoluciones

- i. Audiencia Nacional, Sala de lo Contencioso, Sección 1ª, Recurso 774/2018, de 19 de septiembre de 2019²

¹Resolución de Procedimiento Sancionador N°: PS/00441/2021, Agencia Española de Protección de Datos [ps-00441-2021.pdf \(aepd.es\)](https://www.aepd.es/ps-00441-2021.pdf)

²Audiencia Nacional, Sala de lo Contencioso, Sección 1ª, Recurso 774/2018, de 19 de septiembre de 2019 [Rec 774/2018, 19-09-2019](https://www.audiencia-nacional.es/rec-774-2018)

ii. STJUE C205/21 – Registro de datos biométricos y genéticos
por la Policía

- IV. ***Layered Voice Analysis*. La IA en la entrevista laboral**
- V. **Protección de Datos**
- VI. **Conclusiones**
- VII. **Bibliografía de referencia**

I. *Layered Voice Analysis*. Inteligencia artificial predictiva

LAYRED VOICE ANALYSIS, en adelante (LVA) es una nueva tecnología de análisis de voz. Destacan entre sus principales características los análisis de las señales emocionales, del proceso cognitivo y del estrés en la voz mediante la "actividad de rastreo cerebral" y la "firma emocional". Se configura así una herramienta muy potente, disruptiva respecto de otras soluciones tecnológicas, con aplicaciones en campos tan dispares como puedan ser la criminología, la psicología forense, la psicología, la medicina, etc.

Además de en estos campos, sus particularidades que permiten que pueda emplearse para vincular diferentes rasgos psicológicos con la voz, o detectar y analizar las señales emocionales inconscientes, puede desempeñar un papel determinante para la detección de posibles conductas desviadas, la investigación criminal y la comprensión de las capas de señales emocionales y procesos cognitivos. Como herramienta, hay que tomar en consideración que existen estudios que ponen de relieve las limitaciones y el nivel de azar en el rendimiento de la LVA, principalmente (Manchireddy et al, 2010) y (Conradie, 2007), señalando que cuestiones como la inducción de estrés simulado, el análisis controlado por parte de los operadores de LVA y la falta de cualquier tipo de miedo, incluido el miedo en tiempo real, podría contribuir en los resultados finales. No obstante, esto no merma la potencialidad de la herramienta, muy al contrario, reafirma que la misma tiene por cometido detectar el estado mental actual del hablante, cualquiera que fuera su forma de condicionarlo o generarlo, para detectar su reacción interna a la mentira, sin que en ningún caso se identifique la mentira.

Fijada desde un primer momento la cuestión de las características básicas de la herramienta, es preciso detenerse en una cuestión trascendental, que no es otra que despejar la incógnita de si esta herramienta lo es de Inteligencia Artificial o se trata de una aplicación de automatización.

Desde el momento en que se establecen un conjunto de reglas que, aplicadas sistemáticamente a unos datos adecuados, resuelven un problema cierto, surgen los algoritmos. Actualmente, ese algoritmo se incorpora a una herramienta informatizada capaz de asumir un volumen de gestión de la información y tratamiento de datos inasumible para el ser humano. El desarrollo de la ciencia informática junto con la variable que supone el algoritmo ha terminado por generar la denominada Inteligencia Artificial (en adelante, IA).

La IA existe por cuanto hay máquinas capaces de percibir su entorno y, en consecuencia, llevar a cabo acciones que maximizan sus posibilidades de éxito en los objetivos marcados. Este concepto se usa para referirnos a una máquina, programada para ello, imita las funciones cognitivas propias de los seres humanos, con capacidad de interpretar correctamente datos externos, aprender de ellos y emplear el conocimiento adquirido para alcanzar metas concretas a través de la adaptación flexible (incorporando los nuevos datos obtenidos).

El control de sistemas, la planificación automática, la habilidad de responder a diagnósticos y a consultas de los consumidores, reconocimiento de escritura y del habla... están integrados ya en nuestra realidad diaria. Campos como la economía, la medicina, la ingeniería, el transporte, las comunicaciones y la defensa, entre otros, no se entienden sin la presencia de la IA (incluso el ocio se ha visto imbuido de ésta, a través de distintas aplicaciones de software presentes en juegos de estrategia).

En definitiva, lo que caracteriza a la IA es la posibilidad de que las máquinas aprendan de su propia experiencia, al tiempo que se ajustan a contribuciones nuevas y llevan a cabo tareas. Podemos dividir la IA en dos grupos: por un lado, estarían aquellas que únicamente emplean la lógica, en contraposición de las que además recurren a la intuición. El segundo tipo recibe el nombre de "redes neuronales artificiales" que, al igual que las primeras, funcionan con algoritmos,

pero diseñados como si se tratara de neuronas humanas, para que la máquina aprenda por sí sola (coloquialmente son conocidas como “Deep learning”), creando nuevos algoritmos y produciendo procesos de aprendizaje a partir de los resultados que obtienen.

Con carácter general, la Inteligencia Artificial predictiva es un método de análisis de datos que permite predecir y anticipar las necesidades o eventos futuros de una organización, en distintos frentes tales como marketing, manejo de inventario, logística, ventas, finanzas y mantenimiento de equipos entre otros. Esta tecnología también puede simular un conjunto de escenarios para afinar la estrategia de la compañía, por ejemplo, a nivel de precios, promociones y surtido, por mencionar solo algunos.

Con el aprendizaje automático (machine learning) es posible predecir, simular y automatizar distintos aspectos del manejo financiero de una empresa, entre ellos, los Recursos Humanos. Este modelo predictivo “aprendido” se usa en los datos actuales para proyectar lo que sucederá a continuación, o para sugerir acciones a tomar para obtener resultados óptimos (conveniencia de contratar a un perfil u otro de trabajador). Estas soluciones permiten acelerar el proceso de pronóstico, manejar una gran cantidad y variedad de datos, así como también mejorar continuamente la precisión, creando un sistema robusto.

Naturalmente, siempre habrá factores periféricos que distorsionen los datos, pero, cuantas más fuentes de datos tenga la empresa (internas o externas), más precisas serán sus predicciones cuando se utilice inteligencia artificial y análisis predictivo. Con el aprendizaje automático, las empresas pueden procesar más datos de más fuentes y realizar consultas más complejas y sofisticadas de esos datos, produciendo pronósticos más precisos más rápido.

La tecnología objeto de este informe, el LAYERED VOICE ANALYSIS es una técnica que analiza los rasgos de la voz para determinar la presencia o ausencia de indicadores emocionales, psicológicos o cognitivos en la persona que habla. La idea es que, al analizar ciertos patrones de entonación y ritmo en la voz, se puedan inferir características de la personalidad, emociones o posibles mentiras. LVA utiliza un software que procesa las grabaciones de voz y las analiza en varias capas, evaluando diferentes características del habla y la voz. Esta técnica puede ayudar en la detección de engaños (aunque directamente no determina la existencia de una mentira), identificar patrones de estrés, depresión, ansiedad y otros indicadores psicológicos.

Aplicada al ámbito de Recursos Humanos y Seguridad, principalmente en las áreas de precalificación de empleo, seguimiento para empleados y creación de perfiles, entre sus posibles ventajas, destaca por la rapidez con que se realiza la prueba (en unos 30 minutos aprox.), con una fiabilidad superior al 80%, sin necesidad de intervención humana durante su desarrollo, siendo muy sencilla la capacitación de sus operadores.

Una vez seleccionado el tipo de prueba y calibrado el sistema, se informa al candidato de cómo se va a desarrollar la prueba. Las preguntas aparecen en la pantalla, a medida que el usuario va respondiendo y el propio sistema informa del final de la entrevista. Los resultados pueden analizarse en el momento o realizar varias entrevistas de forma continua y generar un reporte final.

Estas particularidades, determinan que la herramienta LVA es un sistema de IA básico, en el sentido en que no adopta en si misma una decisión, si no que detalla resultados, que deben ser aplicados por el decisor que no es la herramienta. Esto lo aproxima, con los efectos regulatorios propios, a un sistema de automatización, que, si bien obviamente es IA, supone centrar el informe en las cuestiones

regulatorias propias de los procesos de automatización, salvo cuando la normativa no diferencie entre niveles de IA.

II. Regulación y límites

La cuestión de la regulación de la IA, debemos abordarla desde una perspectiva amplia, ya que la tecnología en si no es posible regularla, pudiendo hacerlo respecto de aplicaciones o partes concretas, incluso hasta el punto de la prohibición de uso, al menos temporal, como ha ocurrido por ejemplo con el chatbot inteligente ChatGPT (tecnológica estadounidense OpenAI) en Italia, por no cumplir con la normativa de privacidad.

En España existen diferentes disposiciones en proceso para regular las circunstancias que rodean a esta tecnología. Ejemplo de ello es el Anteproyecto de Ley de Regulación de la Inteligencia Artificial, que establece un mecanismo de supervisión y cumplimiento de la normativa en IA, garantizando la seguridad y la ética mediante la Agencia Española de Evaluación y Certificación de la IA.

Los algoritmos usados en la IA potencialmente causarán discriminación, exclusión y desigualdades, incluso podrán suponer una amenaza para la diversidad cultural, social o biológica, debido a los sesgos humanos que se incorporan en su programación, además del posible uso indebido, malicioso o abusivo. Es importante tener en cuenta estas circunstancias y promover la transparencia en el desarrollo y uso de la IA, para dirigir estos nuevos sistemas hacia un uso ético y responsable, evitando el impacto negativo en los derechos humanos.

La IA supone actualmente una de las tecnologías más avanzadas y, a la vez, comprometedoras. Si bien es útil para mejorar el sistema social, económico, automovilístico, sanitario o educativo, no se pueden perder de vista los riesgos que entraña la automatización de los equipos especialmente al entrar en conflicto con los derechos de intimidad y protección de datos. Los algoritmos usados en la IA

están causando un importante retroceso de las libertades y de la igualdad real de los ciudadanos; orientan y predicen la decisión humana, cuando no la adoptan por sí mismos directamente siendo cada vez más autónomos y disminuyendo con ello la capacidad de controlarlos. La Asociación de Auditoría y Control de Sistemas de Información³ afirma la necesidad de "regular y legislar acerca de los límites éticos del uso de tecnologías disruptivas como la algoritmia, la inteligencia artificial y el aprendizaje de máquinas generativo", de manera que se protejan los intereses generales de la sociedad.

Existen diferentes posiciones respecto del grado de vulneración de derechos fundamentales como la intimidad en relación al uso de la IA, lo que influye tanto en las medidas preventivas adoptadas como en las condiciones impuestas para su uso. En el primer caso, Italia, como ya adelantábamos, ha sido el primer país europeo en prohibir el uso del sistema de IA Chat GPT por vulnerar la privacidad de los usuarios, al permitir acceder a los títulos de las conversaciones de otros usuarios. Además, el Garante italiano para la Protección de Datos Personales afirma que *"no hay una base legal que sustente la recopilación y el procesamiento masivos de datos personales para entrenar a los algoritmos en los que se basa la plataforma"*, así como la ausencia de controles para evitar su uso por parte de menores, lo que vulneraría además la protección a la infancia.

Aquí el problema que nos encontramos es el uso de las aplicaciones, entre ellas LVA. Es decir, no se proscribe en sí misma a la IA, si no que se hace lo propio con determinadas herramientas o aplicaciones de ésta. En cuanto a las condiciones de uso en ciertos casos, puede destacarse la sentencia STS 163/2021, que concluye que la geolocalización de los trabajadores de reparto de comida a domicilio a través de sus propios teléfonos móviles invade el derecho a la privacidad de sus datos, pese a obedecer a un "fin legítimo" relacionado con la tendencia comercial

³ Ver más en [In Pursuit of Digital Trust | ISACA](#)

de la competencia, pero no supone una invasión en su intimidad si el dispositivo utilizado para ello es propiedad de la empresa. Esta sentencia sucede al recurso de casación presentado contra la Sentencia de la Sala de lo Social de la Audiencia Nacional 13/2019, en la que se expresa:

“Califica la geolocalización como tratamiento de datos personales, y concluye que el uso para tal fin de un dispositivo de propiedad de los trabajadores, no ya la geolocalización en sí, vulnera el derecho a la intimidad de los trabajadores, por no superar el juicio de proporcionalidad, ya que esta podría realizarse con mecanismos de ubicación de los vehículos de reparto que no impliquen cesión de datos personales, y por no respetar los deberes informativos que en materia de gestión de datos personales impone la legislación de protección de datos, tanto la que debe proporcionarse a los trabajadores como a su representación legal”.

Más aplicable a las particularidades de LVA es el **Libro Blanco sobre la inteligencia artificial** donde se explica que **la recopilación y el uso de datos biométricos**, en tanto que puede servir para la identificación remota, **entraña riesgos específicos para los derechos fundamentales, por lo que se debe prestar especial atención a las circunstancias específicas que puedan justificar dicho uso**. Sin ir más lejos, a nivel europeo, la Opinión Conjunta 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo, por el que se establecen las normas armonizadas sobre IA, el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos, solicitan una prohibición general de cualquier uso de la IA para un reconocimiento automático de las características humanas en espacios de acceso público (caras, huellas dactilares, voz, pulsaciones de teclas...) en cualquier contexto:

*«...Recomiendan la prohibición, **tanto para las autoridades públicas como para las entidades privadas**, de los sistemas de IA que clasifican a las personas a partir de datos biométricos (por ejemplo, el reconocimiento facial) en grupos por razón de su origen étnico, sexo, orientación política o sexual u otros motivos de discriminación*

prohibidos en virtud del artículo 21 de la Carta, o los sistemas de IA cuya validez científica no está demostrada o que están en conflicto directo con los valores esenciales de la UE [por ejemplo, el polígrafo...»

- **Reglamento europeo sobre el uso de Inteligencia Artificial**

Siguiendo con la normativa europea, sin que exista un texto definitivo aprobado, **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) y se modifican determinados actos legislativos de la Unión COM/2021/206 final**, las bases del futuro Reglamento sobre el uso de Inteligencia Artificial, publicadas por la Comisión Europea, buscan generar el marco europeo adecuado para el control y uso seguro de la IA en Europa. El Reglamento se basa en el riesgo que puede comportar cada sistema de IA, categorizándolos en 4 niveles de riesgo:

- **Riesgo inadmisibles**

Quedarán prohibidos los sistemas de IA considerados amenaza para la seguridad, derechos de las personas o sus medios de subsistencia. Esta prohibición incluye cualquier sistema de IA que manipule el comportamiento de las personas para evitar o condicionar su voluntad, especialmente en caso de menores.

- **Riesgo alto**

Se analizará el potencial lesivo en relación a la salud, seguridad y derechos fundamentales de las personas y las finalidades del sistema en cuestión. Se considerarán sistemas de alto riesgo los usados en

- Infraestructuras críticas
- Formación educativa o **profesional, si pueden usarse para determinar el acceso a la educación y carrera profesional.**

- Servicios esenciales, públicos y privados
- Administración de justicia y procesos democráticos
- Derecho de asilo, movimientos migratorios y gestión de fronteras

Como requisito previo a la comercialización de estos sistemas, se exige la existencia de medios de evaluación y control de riesgos, análisis de los datos que se ingresan al sistema para evitar sesgos discriminatorios, registro de actividad y medidas de supervisión humana. Además es crucial la información al usuario, tanto de estar siendo sometido al sistema como de los objetivos y efectos que se conseguirán.

En la citada Opinión conjunta 5/2021, el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos se acogen con satisfacción que los sistemas de IA que plantean un riesgo elevado deban someterse a una evaluación ex ante de la conformidad antes de poder ser introducidos en el mercado o puestos en funcionamiento en la UE. En principio, se acoge con satisfacción este modelo regulador, ya que ofrece un buen equilibrio entre la facilidad para la innovación y un alto nivel de protección proactiva de los derechos fundamentales. Para poder utilizarlo en entornos específicos, como la toma de decisiones en instituciones de servicio público o infraestructuras críticas, deberán establecerse mecanismos de investigación del código fuente completo.

Sin embargo, el CEPD y el SEPD abogan por adaptar el procedimiento de evaluación de la conformidad previsto en el artículo 43⁴ de la propuesta a fin de

⁴El Art. 43 del citado texto legal expresa que *"Deben aplicarse a los sistemas de IA de alto riesgo requisitos referentes a la calidad de los conjuntos de datos utilizados, la documentación técnica y el registro, la transparencia y la comunicación de información a los usuarios, la vigilancia humana, la solidez, la precisión y la ciberseguridad. Dichos requisitos son necesarios para mitigar de forma efectiva los riesgos para la salud, la seguridad y los derechos fundamentales, según corresponda en función de la finalidad prevista del sistema, y no se dispone razonablemente de otras medidas menos restrictivas del comercio, con lo que se evitan restricciones injustificadas de este"*. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206>

que, por lo general, se lleve a cabo una evaluación ex ante de la conformidad por parte de terceros para la IA de alto riesgo. Aunque la evaluación por terceros de la conformidad para el tratamiento de datos personales de alto riesgo no es un requisito del RGPD ni del RPDUE, aún no se comprenden del todo los riesgos que plantean los sistemas de IA, de ahí que se busque reforzar la seguridad jurídica y la confianza en los sistemas de IA de alto riesgo, incluyendo la obligación general de evaluación de conformidad por terceros.

- **Riesgo limitado**

Se encuadran aquí sistemas donde la persona interactúa con la máquina, entrenada para detectar emociones. Es necesario que el proveedor cumpla ciertas obligaciones de transparencia, además de informar al usuario de que está interactuando con este tipo de sistema, permitiéndole tomar una decisión informada sobre si quiere o no continuar.

- **Riesgo mínimo**

Se trata de sistemas más inofensivos, como filtros de correo electrónico para evitar cierto tipo de mensajería (spam, promociones...). El riesgo que representan para los derechos fundamentales o la seguridad de las personas es nulo, por lo que se obvia la intervención en este caso.

El caso particular de LVA estaría en el nivel de **RIESGO ALTO y en el de RIESGO LIMITADO, correspondiendo, por tanto, aplicar los niveles de control específicos. En particular, los propios del RGPD.** Así el art. 22.2 RGPD dispone que "todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar". La excepción basada en el consentimiento explícito del interesado, no exime al responsable del tratamiento de adoptar "las medidas adecuadas para salvaguardar

los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión”.

Teniendo en cuenta que la voz es un dato biométrico⁵, nos lleva a la interrelación del art. 22.4 con el art. 9, ambos del RGPD. Así las decisiones basadas únicamente en el tratamiento automatizado, no se podrán adoptar si se basaran únicamente en las categorías especiales de datos personales, las cuales están contempladas en el art. 9.1, salvo que se aplique el art. 9. 2, letra a) o g), siempre que se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Es decir que salvo que medie el consentimiento explícito del interesado para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición de uso de estos datos no puede ser levantada por el interesado, o bien, que el tratamiento resulte necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado, no se podrá desarrollar la aplicación LVA en el territorio de la UE.

Dicho de otro modo, lo más sencillo es que, aplicada a la selección de personal, la herramienta LVA no constituya por si sola la única *ratio decidendi* que fundamente la decisión de contratar o dejar de hacerlo.

⁵El art. 4.14 RGPD considera como “datos biométricos” a los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre las que evidentemente se encuentra la voz.

Toda decisión que se fundamente principal o exclusivamente en el uso de sistemas de IA debe tener como presupuesto de su admisibilidad jurídica, la posibilidad de que pueda ser discutida la lógica humana en que se fundamenta. Por ello es requisito imprescindible que la existencia de este presupuesto sea pública. Ni tan siquiera sería suficiente con la posibilidad de conocer la existencia, en tanto no se positive, no hará posible que pueda ser objeto de examen.

La transparencia, la responsabilidad, la previsibilidad, la igualdad ante la ley, incluso la coherencia, se cumplen en tanto imperen ciertas reglas, siendo válida la tecnología específica implementada a su tenor. Pero la rápida evolución de la IA, produce, obsérvese que hablamos en términos de presente, que los algoritmos se integran cada vez más en procesos opacos de toma de decisiones, sin intervención humana, lo que hará que sea extremadamente difícil desafiarlos, con la evidente pérdida de garantías que ello supone. El grado de sofisticación de la automatización que se implementa debe considerarse cuidadosamente.

Si bien puede parecer tentador automatizar completamente un proceso o decisión para lograr una mayor eficiencia y reducir el costo humano asociado, esta decisión debe ser evaluada cuidadosamente en términos de sus impactos potenciales, ya que puede producir resultados impredecible e indeseados. Por lo tanto, es importante considerar los elementos a través de los cuales se diseña una regla específica que confiere poder de decisión al sistema de IA, evaluando los riesgos y consecuencias vinculados a la automatización total de decisiones. También deben ser previstos aspectos como la transparencia, la responsabilidad y la supervisión humana adecuada para garantizar que los resultados sean éticos y justos.

- **Plan nacional de Desarrollo de la IA en China**

La Administración del Ciberespacio de China ha publicado un proyecto para regular los servicios de IA presentes en el país, Medidas Administrativas para los Servicios

de Inteligencia Artificial Generativa, permitiendo un período de información pública y recogida de sugerencias⁶. No obstante China ya cuenta con un conjunto claro de normas dirigidas a la gobernanza de la IA, así el "Reglamento sobre la Evaluación de la Seguridad de los Servicios de Información en Internet con Atributos de Opinión Pública o Capacidades de Movilización Social" y las "Recomendaciones de Algoritmos del Servicio de Información de Internet", como el "Reglamento de Gestión" para llevar a cabo los procedimientos de presentación, modificación y presentación de cancelación de algoritmos, configuran un entorno normativo

Su ámbito de aplicación, de igual forma que las regulaciones europeas, obliga a cualquier prestador de servicios de IA dentro del territorio Chino.

Entre los requisitos que impone a los sistemas de IA generativa se encuentra:

- En el proceso de diseñar los algoritmos y carga de datos, deben tomarse medidas que prevengan la discriminación basada en la raza, étnica, ocupación...
- **Deben aplicarse mecanismos que permitan generar información veraz y exacta, respetando los intereses legítimos de las personas**
- El contenido generado por IA deberá estar debidamente identificado, según el Reglamento de Gestión de Síntesis Profunda del Servicio de Información de Internet.

Antes de comenzar a comercializar estos servicios, se debe solicitar una evaluación de seguridad que pruebe la verificación real de los usuarios y las medidas de protección de datos personales de que disponen. Además, recae

⁶ "Medidas Administrativas para los Servicios de Inteligencia Artificial Generativa (Borrador para Comentarios)", texto disponible en http://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm

en los proveedores la responsabilidad de comprobar la legitimidad de los datos usados para entrenar a estos sistemas.

El 29 de septiembre de 2021, la Administración del Ciberespacio de China, el Departamento de Publicidad del Comité Central del PCCh y otras siete autoridades hicieron pública de forma conjunta el documento "Opiniones orientadoras sobre el fortalecimiento de la gobernanza integral de los algoritmos del servicio de información de Internet" (en adelante, "las opiniones orientadoras", 关于加强互联网信息服务算法综合治理的指导意见)⁷. Estas directrices tienen como finalidad establecer gradualmente el patrón de gobernanza integral de la seguridad algorítmica en unos tres años.

En términos de gobernanza algorítmica, las opiniones orientadoras enfatizan la necesidad de aclarar más los derechos, obligaciones y responsabilidades del gobierno, las empresas, las organizaciones industriales y los cibernautas en la gobernanza de la seguridad de los algoritmos, y fortalecen las responsabilidades de las entidades de las empresas y la regulación de las organizaciones industriales.

En ese sentido, las principales disposiciones que las directrices incluyen y que deben ser aplicadas por dichas empresas son:

- Brindar a los usuarios mayor transparencia sobre cómo operan sus algoritmos de recomendación, incluida toda información sobre cuándo se utilizan los sistemas de recomendación de una empresa y los «principios, intenciones y mecanismos de operación» básicos de cada sistema.
- Permitir que se monitoree y audite sus algoritmos, incluidos los modelos, los datos de capacitación y los resultados de forma regular.

⁷http://www.gov.cn/zhengce/zhengceku/2021-09/30/content_5640398.htm

- Contar con un proceso de registro y establecimiento de un equipo técnico para evaluar los mecanismos y riesgos de algún algoritmo.
- Dar a los usuarios la opción de desactivar las recomendaciones algorítmicas u optar por no recibir recomendaciones basadas en sus perfiles.
- Permitir que los usuarios determinen si la empresa puede utilizar sus datos para desarrollar y operar sistemas de recomendación. Más aún, si un usuario cree que el algoritmo de recomendación de una plataforma ha tenido un impacto negativo en sus derechos, puede solicitar que la plataforma proporcione una explicación de su decisión al usuario. En estos casos, el usuario también puede exigir que la empresa realice mejoras en el algoritmo.

- **Estados Unidos**

En la misma forma que China, Estados Unidos también ha abierto un período de consulta pública sobre su proyecto de regulación de la IA⁸. A pesar de que ésta tecnología puede tener un impacto positivo en sectores económicos y sociales, también comporta riesgos que deben ser tenidos en cuenta. La adopción de estos sistemas dependerá de la confianza y aceptación que demuestre la sociedad hacia ellos.

El proyecto estadounidense incluye diferentes ítems a tener en cuenta, entre ellos:

- Confianza social en la inteligencia artificial
- Participación pública
- Integridad científica y calidad de la información

⁸Vough, R. T. (2019) Memorandum For The Heads Of Executive Departments And Agencies on "Guidance for Regulation of Artificial Intelligence Applications". Disponible en: [2019-CATS-5830-REV_DOC--DraftOMBMemoonRegulationofAI101019.docx](https://www.whitehouse.gov/wp-content/uploads/2019/03/2019-CATS-5830-REV_DOC--DraftOMBMemoonRegulationofAI101019.docx) ([whitehouse.gov](https://www.whitehouse.gov))

- Evaluación y gestión de riesgos
- Costes y beneficios
- Flexibilidad
- Equidad y no discriminación
- Divulgación y transparencia
- Seguridad
- Coordinación entre Agencias

Todos estos aspectos deberán cumplirse y ser tenidos en cuenta antes de la comercialización de cualquier sistema basado en IA, además de la cooperación internacional:

"Por consiguiente, las agencias deberían entablar diálogos para promover enfoques regulatorios consistentes sobre la inteligencia artificial que fomenten la innovación en la inteligencia artificial estadounidense al tiempo que protejan la privacidad, los derechos civiles, las libertades civiles y los valores estadounidenses. Dichas discusiones, incluidas las que se lleven a cabo con el público en general, pueden brindar valiosas oportunidades para compartir las mejores prácticas, datos y lecciones aprendidas, y asegurar que Estados Unidos siga siendo líder en el desarrollo de la inteligencia artificial."

Conviene tener presente en el caso particular de EEUU la "Clarifying Lawful Overseas Use of Data Act" conocida como "CLOUD Act". El objetivo de esta norma es agilizar ciertas investigaciones, cuando estas requieren acceder a servidores o nubes alojadas fuera de EEUU, pero que pertenecen a proveedores estadounidenses, como es el caso, por ejemplo, de Microsoft, Amazon o Google. Es preciso resolver las dudas que, sobre los usuarios de estas mismas entidades, o cualquier otra norteamericana, radicados fuera de EEUU, respecto al alcance de esta ley en esos terceros países. Así si la empresa a la que se le pide acceso a sus datos es norteamericana, aunque estos estén alojados en un servidor o nube alojada en Europa, por la Cloud Act, si recibe una orden judicial para ello, tendrá

que conceder dicho acceso (existe la posibilidad de negarse, pero es un procedimiento complejo y de consecuencias impredecibles). En caso de que la empresa fuera europea o de otra nacionalidad no EEUU, la Cloud Act no le será de aplicación.

Desde febrero de 2022 EEUU cuenta con una propuesta en la Cámara de Representantes de Estados Unidos de un proyecto de Ley de Responsabilidad Algorítmica⁹. Bajo la premisa de mejorar la transparencia, la rendición de cuentas y la equidad de las decisiones automatizadas p. ej., en el acceso a la universidad o en la obtención de préstamos bancarios, con afectación directa en los ciudadanos, la norma, en fase de aprobación, exigiría tanto a la empresa que toma las decisiones como a la entidad que desarrolle la tecnología algorítmica que realicen evaluaciones de impacto en cuanto a sesgo, eficacia y otros factores.

- **Arabia Saudí**

La política y los procedimientos de privacidad saudí se rigen por la ley de protección de datos personales (Real Decreto (M/19) de fecha 1443/2/9 AH)¹⁰, los Principios Básicos de Protección de la Información Personal y los Principios Básicos y Normas Generales para Compartir Datos emitidos por la Autoridad Saudí de Datos e Inteligencia Artificial (SDAIA) y la Oficina Nacional de Gestión de Datos (NDMO)¹¹, que remiten a la normativa de privacidad la gestión de la información que se gestione por las aplicaciones que empleen IA.

La Ley de Protección de Datos Personales y sus reglamentos ejecutivos establecen la base jurídica para la protección de sus derechos en relación con el tratamiento de datos personales por parte de todas las entidades del Reino, así como de todas

⁹<https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202022%20Bill%20Text.pdf>

¹⁰Disponible en <https://sdaia.gov.sa/en/SDAIA/about/Pages/RegulationsAndPolicies.aspx>

¹¹<https://sdaia.gov.sa/en/default.aspx>

las entidades fuera del Reino que traten datos personales relacionados con personas físicas residentes en el Reino utilizando cualquier medio, incluido el tratamiento de datos personales en línea, lo que incluye los sistemas de automatización y los de IA.

Los principios fundamentales de la política de protección de datos, que no se separan en lo esencial de las regulaciones de los estados ya analizados, incluyen:

- Responsabilidad del responsable de la entidad (o de la persona que éste designe) sobre las políticas y procedimientos de privacidad del Responsable del Tratamiento.
- Transparencia a través del Aviso de Privacidad indicando los fines para los que se recogen los datos personales.
- Elección y consentimiento obtenidos mediante la aprobación implícita o explícita de la recogida, uso y divulgación de los datos personales antes de su recogida.
- Limitación de la recogida de datos al mínimo que permita el cumplimiento de los fines.
- Uso, Conservación y Destrucción estrictamente para los fines previstos, conservados durante el tiempo necesario para lograr los fines previstos o según lo exijan las leyes y reglamentos y destruidos de forma segura, evitando fugas, pérdidas, robos, usos indebidos o accesos no autorizados.
- Acceso a los datos mediante el cual cualquier interesado puede revisar, actualizar y corregir sus datos personales.
- Limitación de divulgación de datos aprobada por el Titular de los datos restringe a terceros a los fines previstos en el Aviso de privacidad.
- Seguridad de los datos mediante la protección de los datos personales contra fuga, daño, pérdida, robo, mal uso, modificación o acceso no

autorizado; conforme a los controles emitidos por la Autoridad Nacional de Ciberseguridad y demás autoridades competentes.

- Calidad de los datos previa verificación de su exactitud, integridad y oportunidad.

Seguimiento y cumplimiento de las políticas y procedimientos de privacidad del Responsable del Tratamiento, así como de cualquier consulta, reclamación o litigio relacionado con la privacidad.

- **México**

En fase de elaboración, la norma mexicana futura vendrá definida por su propio rótulo, el cual ya es significativo en cuanto la línea regulatoria que probablemente desarrolle el texto final. El proyecto de "Ley para la regulación ética de la Inteligencia Artificial para los Estados Unidos Mexicanos"¹², busca crear estructuras y apuntar hacia estándares éticos de creación, investigación y uso de la IA en el país, así como crear y regular un Consejo Mexicano de ética para la Inteligencia Artificial y la Robótica (CMETIAR).

Hasta la aprobación del texto específico, la IA en México es preciso abordarla desde la perspectiva de la protección de datos personales. A esos efectos, la referencia normativa es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Nueva Ley publicada en el Diario Oficial de la Federación el 5 de julio de 2010)¹³, desarrollada por el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares¹⁴.

Texto ciertamente obsoleto hoy en día, ajeno a la evolución tecnológica, no deja, sin embargo, de resultar aplicable, por cuanto regula el tratamiento de datos

¹² <http://gaceta.diputados.gob.mx/Gaceta/65/2023/mar/20230330-III.html>

¹³ <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

¹⁴ https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

personales, aunque omita los de carácter biométrico estricto sensu, habrá que entenderlos comprendidos en el compendio del art. 3 V y VI de la Ley como datos personales, en particular datos personales sensibles, con el tratamiento correspondiente basado en el consentimiento informado del interesado.

- **Brasil**

El texto de referencia es la Lei Nº. 13.709, de 14 de agosto de 2018 Lei Geral de Proteção de Dados Pessoais (LGPD), (Redação dada pela Lei nº 13.853, de 2019)¹⁵. Ya su artículo 1, dispone que *este texto regula el tratamiento de datos personales, **incluso en soporte digital**, por personas físicas o jurídicas de derecho público o privado, con el fin de proteger los derechos fundamentales a la libertad y a la intimidad y el libre desarrollo de la personalidad de las personas físicas.*

En relación con el tratamiento automatizado de datos, el artículo 20, determina que *el interesado tendrá **derecho a solicitar la revisión de las decisiones adoptadas exclusivamente sobre la base de un tratamiento automatizado de datos personales** que afecten a sus intereses, incluidas las decisiones destinadas a definir su perfil personal, profesional, de consumo y de crédito o aspectos de su personalidad*¹⁶.

Para dar cumplimiento a esa revisión de forma efectiva, el responsable del tratamiento facilitará, siempre que se le solicite, información clara y adecuada sobre los criterios y procedimientos utilizados para la decisión automatizada, teniendo debidamente en cuenta los secretos comerciales e industriales (art. 20.1).

En caso de que no se facilite la información a que se refiere el epígrafe preterido, aunque se oponga un argumentario basado en la observancia de secretos

¹⁵ http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm

¹⁶En su redacción dada por la Ley 13.853 de 2019).

comerciales e industriales, la autoridad nacional podrá llevar a cabo una auditoría para verificar aspectos discriminatorios en el tratamiento automatizado de datos personales¹⁷.

A diferencia de la normativa mexicana, la brasileña refiere expresamente a los datos biométricos, confiriéndoles el nivel de dato personal sensible, amparándolo con el máximo nivel de protección.

- **Irak**

El texto de referencia iraquí es su Constitución de 2005 (vigente a la fecha), la cual en su artículo 17.1º, dispone que toda persona tiene el derecho en la privacidad en la medida de que no vaya en contra del derecho de los demás o de la moral pública. De igual modo, su artículo 40 garantiza la libertad de comunicación y de correspondencia postal, telegráfica, telefónica, electrónica u otras, de modo que no pueden ser objeto de espionaje, de escucha o de publicación, excepto en casos de necesidad judicial y de seguridad y por decisión judicial.

Con una normativa dispersa, la Law on Freedom of Expression of Opinion, Assembly, and Peaceful Demonstration, de mayo de 2011, desarrolla los preceptos constitucionales en este ámbito, pero es una realidad distorsionada por normas como la Ley de Delitos de la Información de Irak que ha tenido manifestaciones como el corte de Internet a la población ya que criminaliza actividades legítimas como compartir información y establecer contactos.

En un marco jurídico inestable, cualquier iniciativa deberá ser contrastada previamente con las autoridades para garantizar, en medida de lo posible, la viabilidad de su uso, conforme al Islam religión oficial del Estado y principal fuente

¹⁷La referencia a la autoridad nacional hay que entenderla hecha a la Autoridade Nacional de Proteção de Dados (ANPD).

de la legislación, como reconoce la propia Constitución, dejando en un papel muy debilitado cualquier situación no amparada por la Sharía.

III. Consideraciones legales sobre el análisis de datos biométricos. Jurisprudencia y resoluciones al respecto

El uso de aplicaciones de IA para la identificación biométrica es cada vez más frecuente, mientras que el marco regulatorio es insuficiente. Las operaciones biométricas pueden emplear distintas técnicas, algunas de forma simultánea. Las técnicas de proceso de datos biométricos se basan en recoger y procesar rasgos físicos, conductuales, fisiológicos o neuronales, mediante dispositivos o sensores, creando patrones que posibilitan la identificación, seguimiento o perfilado de las personas.

Algunos métodos requieren la cooperación de la persona, mientras que otros pueden capturar datos biométricos a distancia, sin que el individuo pueda tener consciencia de ello. Existen ciertos criterios de clasificación de los sistemas biométricos (tecnologías diferentes, dispositivos o sensores, rasgos estudiados...), sin embargo, a la hora de demostrar la adecuación de estas técnicas al Reglamento General de Protección de Datos y de evaluar el riesgo para los derechos y libertades de las personas, es conveniente emplear criterios de clasificación de las operaciones biométricas desde el punto de vista de la protección de datos.

En el caso de LAV evidentemente es indispensable la cooperación de la persona para la obtención de los datos, pero en esencia este extremo no va a afectar a la cuestión regulatoria, más allá de lo referente a la recabación y gestión del consentimiento del titular de los datos.

- **Resoluciones de la Agencia Española de Protección de Datos**

La AEPD, como encargada de velar por el cumplimiento de la normativa española y europea de protección de datos de carácter personal, supervisa el tratamiento de dichos datos por parte de las entidades y empresas que operan en España. Entre otras funciones, se encarga de la imposición de sanciones y medidas correctivas en caso de infracciones a la normativa. En los últimos años, ha publicado varias resoluciones sancionadoras en relación con la inteligencia artificial y el tratamiento de los datos personales, hemos destacado aquellas que guardan una relación directa con el objeto del presente informe, por entenderlas de especial trascendencia para cuanto se recoge en el mismo.

- Mobile World Congress – Expediente 202100603,

La AEPD propone una multa de 200.000,00€ a GSMA LIMITED¹⁸, empresa organizadora del congreso Mobile World Congress en el año 2021. La resolución se basa en la denuncia de una ciudadana británica, asistente al evento, sobre la necesidad de proporcionar una fotografía de su pasaporte para poder acceder al recinto, sin tener constancia cierta del tratamiento posterior que se realizaría de dicha información. La política de privacidad de GSMA (con sede en Bielorrusia) indicaba la posible cesión de datos a terceros países, extremo que fundamenta la reclamación de la denunciante.

La resolución reza lo siguiente:

"A.A.A – la denunciante - Fue invitada como ponente en la edición del MOBILE WORLD CONGRESS, (MWC) de junio 2021, celebrado en Barcelona. Con tal fin, se daba la opción de registrarse para el evento en "virtual", o

¹⁸Resolución de Procedimiento Sancionados, Exp202100603, Agencia Española de Protección de Datos. <https://www.aepd.es/es/documento/ps-00553-2021.pdf>

“presencialmente”. Para la opción en “presencial”, “la reclamada solicita cargar datos de categoría especial-detalles del pasaporte, incluyendo fotografías que se transfieren a un encargado situado en un país tercero-, para el reconocimiento facial con fines de seguridad”.

Manifiesta que la política de privacidad (<https://www.mwcbarcelona.com/>), “establece que la base del tratamiento es el consentimiento, sin embargo, en correo electrónico se ha declarado que se basa en el artículo 6.1 c), del RGPD, es decir, el cumplimiento de una obligación legal, haciendo referencia al artículo 22.2 de la LOPD y al artículo 11.1.h de la Ley Orgánica 2/1986.

No es posible registrarse como ponente presencial sin cargar (subir) datos biométricos. A pesar de intentar solucionar la cuestión para encontrar una alternativa, ha sido necesario cargar mi pasaporte para el registro.” **Considera que no existe obligación legal válida para ese tipo de tratamiento de reconocimiento facial**”.

Así, la resolución recoge que GSMA cometió una infracción del artículo 35 del RGPD, que establece:

“Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, **entrañe un alto riesgo para los derechos y libertades de las personas físicas**, el responsable del tratamiento **realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales**. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares”.

La defensa de GSMA se basa en que se proporcionaba la opción de registro como asistente online, mediante el cual no sería necesaria la fotografía del pasaporte. Por esto, de una u otra forma, la empresa obliga a proporcionar dicha información a aquellos participantes que quieran asistir presencialmente, justificando ello en la situación sanitaria provocada por el Covid-19.

Lo importante en este caso no es el consentimiento, ni la ausencia de alternativa a la facilitación de datos, algo que también ocurriría en el caso de la herramienta LVA. Aquí lo verdaderamente importante es que es **ABSOLUTAMENTE IMPRESCINDIBLE**, además reseñamos especialmente que aplica a todo el ámbito de la Unión Europea la **EVALUACIÓN DE IMPACTO PREVIA A LA ACTIVIDAD**.

Consecuentemente también habrá que desarrollar una **ACTIVIDAD DE TRATAMIENTO ESPECÍFICA** para ese supuesto concreto.

- Consejería de Sanidad de Castilla la Mancha - Expediente N.º: PS/00441/2021¹⁹

Se sanciona a la Consejería de Sanidad de Castilla la Mancha con apercibimiento por infringir el art. 35 del Reglamento General de Protección de Datos. La reclamación, con origen en un proceso solicitando la concesión de permisos de teletrabajo, indica lo siguiente:

“El reclamante... expone que hasta el 13 de marzo de 2020 ha estado fichando con su huella dactilar sin que previamente le hayan informado del uso y finalidad del tratamiento que realizarían con sus datos personales, siendo estos posteriormente utilizados para sancionarle.”

En este sentido, la AEPD solicita:

1. Descripción precisa del funcionamiento del instrumento utilizado para la captación de las huellas dactilares.
2. Criterios utilizados para la codificación y el almacenamiento de la información captada (si los datos biométricos se almacenan en bruto o si son tratados de manera que sólo se almacena una plantilla biométrica).
3. Motivos que justifiquen la necesidad y la proporcionalidad del uso de los datos biométricos para la finalidad perseguida.

¹⁹ Resolución de Procedimiento Sancionador N.º: PS/00441/2021, Agencia Española de Protección de Datos [ps-00441-2021.pdf \(aepd.es\)](https://www.aepd.es/ps-00441-2021.pdf)

4. Medidas adoptadas para garantizar que no es posible la reutilización de los datos biométricos para otra finalidad.”

La parte reclamada, la Consejería de Sanidad de Castilla la Mancha, justifica el uso de un sistema de fichaje mediante huella dactilar en la necesidad de evitar la suplantación de identidad por parte de otros empleados, tras comprobar el mal uso dado a otros sistemas como tarjetas de identificación o códigos personales. Propone además como medida *“optar por sistemas de verificación o autenticación biométrica 1:1, utilizando la fórmula de combinar código más huella en todos los casos. Además, se recomienda que los sistemas se basen en la lectura de los datos biométricos conservados por la persona trabajadora, por ejemplo en una tarjeta”* de manera que se evite la posesión por parte de esta Consejería de los datos biométricos (huellas dactilares en este caso) de sus trabajadores.

La citada Consejería explica además:

A la hora de valorar la implantación de una de estas soluciones, se optó por introducir la identificación con huella dactilar ya que es una forma menos suplantable que las otras. Si se utiliza la huella dactilar, solo puede ser el propio empleado el que acceda al sistema de fichaje. Se decidió tras comprobarse el mal uso que se estaba dando a otros sistemas como tarjetas de identificación o códigos.

Por tanto, no existe ninguna otra medida que permitiera lograr este objetivo con el mismo nivel de eficacia (...) La utilización de la huella es una medida más racional y justa, ya que asegura el momento real en que el empleado ha entrado y salido de su lugar de trabajo.

Además, el evitar posibles incumplimientos horarios por parte de un empleado es importante ya que puede dar lugar a que sean otros compañeros los que tengan que asumir su trabajo. Pese a que el uso de la huella supone un tratamiento más invasivo, los beneficios de este sistema no solo para el empleador sino para el interés público superan los perjuicios para este derecho. Además, el resto de las alternativas, uso de credenciales, de códigos, no impiden que se suplante la identidad del empleado.”

A pesar de la justificación en los términos planteados por la administración autonómica, señala la AEPD que la reclamada continúa utilizando la huella dactilar **sin haber realizado una evaluación de impacto sobre esa operación de tratamiento que entraña probablemente un alto riesgo en los derechos y libertades de los empleados**. Así pues, entre otras cuestiones, **continúan sin identificar los riesgos asociados al tratamiento del uso de la huella dactilar para control horario, y por tanto sin poder mitigarlos, existiendo otras modalidades que para dicho fin tiene instaurada la reclamada**. Se considera pues, con el fin de garantizar los derechos y libertades de los titulares de los datos, que concurre la necesidad y justificación de adoptar poderes correctivos que se determina en la parte dispositiva.

- Mercadona. Procedimiento Sancionador N° PS/00120/2021 sobre reconocimiento facial.

Se sanciona a la empresa Mercadona²⁰ con una multa de 3.150.000€, referente a varias infracciones:

1. Infracción de los arts. 6 y 9 del RGPD – multa administrativa de cuantía 2.000.000 € (dos millones de euros)
2. Infracción de los arts. 12 y13 del RGPD – multa administrativa de cuantía 100.000 € (cien mil euros)
3. Infracción del art. 5.1.c) del RGPD – multa administrativa de cuantía 500.000€ (quinientos mil euros)
4. Infracción del art. 25.1 del RGPD – multa administrativa de cuantía 500.000€ (quinientos mil euros)
5. Infracción del art. 35 del RGPD – multa administrativa de cuantía 50.000€ (cincuenta mil euros).

Según se indica:

²⁰ Procedimiento sancionador N°: PS/00120/2021, Agencia Española de Protección de Datos [PS-00120-2021 Resolución de fecha 23-07-2021 Artículo 12 13 15 25 35 5.1.c\) 6 9 RGPD \(aepd.es\)](#)

“El tratamiento de datos basados en el reconocimiento facial con fines de identificación implantado por MERCADONA se encuentra prohibido por lo dispuesto en el artículo 9.1 del RGPD, al no constar ninguna causa que permita levantar la prohibición entre las expuestas en el art. 9.2 del RGPD, por lo que no procede ampararse en las causas de licitud del art. 6.1 del mismo. Tal prohibición no puede obviarse mediante la aplicación de medidas de seguridad proactiva, ya que la prohibición del tratamiento señalada en el art 9.1 del RGPD determina que sean irrelevantes, por lo que no se procede al análisis de las mismas”.

De esta resolución debemos extraer la **necesidad de justificar debidamente el motivo del uso de la herramienta dejando de forma totalmente clara y determina el porqué de la necesidad de la herramienta, diferenciándola de una entrevista personal (que no comportaría tratamiento de datos biométricos -siempre que no se grabara la misma-.**

- Consulta N/REF: 0098/2022

Se plantea consulta sobre la viabilidad jurídica de la implantación de sistemas biométricos para el control de accesos a gradas de animación, por acuerdo de la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia. Tal medida se fundamenta en el art. 13.1 de la Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte, que faculta para decidir la implantación de medidas adicionales de seguridad en competiciones deportivas de alto riesgo.

La base jurídica de tal medida estaría en el art. 6.1.e) del Reglamento Europeo General de Protección de Datos, 2016/679, que facultaría *“para el cumplimiento de una misión realizada en interés público (garantizar la seguridad e integridad de los asistentes y prevenir la vulneración de derechos fundamentales) o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”*.

Como indica el propio documento:

Asimismo, al referirse la medida solicitada al tratamiento de categorías especiales de datos se aplicaría la excepción regulada en el artículo 9.2.g) del RGPD, es decir, que el tratamiento del dato biométrico “es necesario por **razones de un interés público esencial**²¹, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser **proporcional al objetivo perseguido**, respetar en lo esencial el derecho a la protección de datos y establecer **medidas adecuadas y específicas para proteger los intereses y derechos fundamentales** del interesado.”

Para introducir el mencionado sistema, deberá realizarse con carácter previo un juicio de proporcionalidad, valorando la idoneidad de la medida y la necesidad del tratamiento. Además, debe llevarse a cabo una Evaluación de Impacto en relación a los requisitos marcados por el art. 35 del RGPD.

La respuesta de la AEPD a la consulta planteada determina: en primer lugar, que del art. 13.1 la citada ley 19/2007 no contempla el tratamiento de datos biométricos ni establece garantías para la protección de datos personales; en segundo lugar, el uso de sistemas de identificación biométrica sólo podría llevarse a cabo en virtud de alguna de las circunstancias detalladas en el art. 9.2 de la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, premisa que no se cumple en este caso. Por tanto, concluye que el acuerdo de la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia no cuenta con el rango

²¹ Se cita en la consulta, entre otras, la resolución D. L. contra Bulgaria, núm. 7472/14, de 19 de mayo de 2016: “En relación con lo que debe entenderse por interés público esencial, debe tenerse igualmente en cuenta la Jurisprudencia del Tribunal Europeo de Derechos Humanos, que al amparo del artículo 8 del Convenio Europeo de Derechos Humanos, viene considerando que el tratamiento de datos personales constituye una injerencia lícita en el derecho del respeto de la vida privada y sólo puede llevarse a cabo si se realiza de conformidad con la ley, sirve a un fin legítimo, respeta la esencia de los derechos y libertades fundamentales y es necesario y proporcionado en una sociedad democrática para alcanzar un fin legítimo.

También la sentencia Leander contra Suecia, núm. 9248/81, 26 de marzo de 1987: «el concepto de necesidad implica que la injerencia responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue».

normativo necesario para permitir el uso de dichos sistemas, con lo que estos se consideran contrarios a la normativa reguladora en materia de protección de datos.

- **Otras resoluciones**

- Audiencia Nacional, Sala de lo Contencioso, Sección 1ª, Recurso 774/2018, de 19 de septiembre de 2019²²

Se plantea denuncia ante la AEPD contra el gimnasio QUO Fitness por la introducción de un nuevo sistema de acceso mediante huella dactilar, sin haber informado previamente a sus usuarios ni darles una alternativa en caso de oponerse a la recogida de sus datos biométricos. La entidad denunciada alega no que los datos recogidos no pueden considerarse biométricos, en la medida que no permiten la identificación de la persona.

La sentencia se pronuncia en el siguiente sentido:

“Los datos biométricos pueden considerarse como información sobre una persona física; ya que afectan a datos que proporcionan, por su propia naturaleza, información sobre una persona determinada. Entre los datos biométricos más utilizados se encuentra la huella dactilar y si bien una huella dactilar completa identifica a la persona, también es susceptible de identificarse a la misma persona con la toma de muestras o partes de la huella transformadas en una plantilla, aunque sea a través de un algoritmo, ya que, como razona la resolución recurrida, esas muestras convertidas en algoritmos, mediante su registro en una base de datos, permiten al ser tratados la identificación de la persona cuando acude al gimnasio, a través del proceso de matchmaking (emparejamiento), entrando en el ámbito de dato personal”.

En el caso de LVA, entendiéndolo, como se deduce del análisis expuesto de las resoluciones anteriores la proporcionalidad de la medida que supone el recurso a esta tecnología, no cabe duda que cabría el ejercicio legítimo del derecho de

²²Audiencia Nacional, Sala de lo Contencioso, Sección 1ª, Recurso 774/2018, de 19 de septiembre de 2019 [Rec 774/2018, 19-09-2019](#)

oposición, lo que ocurre es que, de ser así, se estaría renunciando por el interesado a la realización de la entrevista, lo que equivaldría en la práctica a su exclusión del proceso selectivo. No obstante, si el uso de LVA se entiende proporcionado, además cumpliendo con todas las garantías antedichas en cuanto a evaluación de riesgo, tratamiento de datos, etc., en definitiva, adecuado a la normativa más estricta vigente, nada impide que la oposición al tratamiento, con el resultado anunciado, sea totalmente legítima y no pueda aducirse la necesidad de sustituir el uso de LVA por medidas como una entrevista personal, por ejemplo.

- STJUE C205/21 – Registro de datos biométricos y genéticos por la Policía

Establece que *“la recogida sistemática de datos biométricos y genéticos de cualquier persona investigada a efectos de su inscripción en el registro policial es contraria al requisito de garantizar una mayor protección con respecto al tratamiento de datos personales sensibles”*.

Las autoridades policiales búlgaras solicitaron autorización para la recogida forzosa de datos genéticos y biométricos de una detenida, acompañando la solicitud únicamente del auto policial y la declaración de la detenida en la que se opone a la obtención de sus datos.

Se plantea la compatibilidad de la normativa búlgara con la Directiva 2016/680, declarando el Tribunal de Justicia de la Unión Europea²³ que “el derecho nacional autoriza el tratamiento de datos biométricos y genéticos por parte de las autoridades policiales, a efectos de sus actividades de investigación (...) siempre

²³Tribunal de Justicia de la Unión Europea, 26 de enero de 2023. *Sentencia del Tribunal de Justicia en el asunto C-205/21 | Ministerstvo na vatreshnite raboti (Registro de datos biométricos y genéticos por la Policía)*. Comunicado de prensa 16/23. Disponible en: europa.eu

que ese Derecho contenga una base jurídica suficientemente clara y precisa que lo autorice”.

La citada Directiva 2016/680 permite el tratamiento de datos sensibles, como puedan ser los biométricos o los genéticos, por parte de las autoridades para fines de prevención siempre que sea estrictamente necesario y revestido de las garantías adecuadas, además de previsto por la normativa europea o nacional. A este respecto, la normativa búlgara establece:

“En caso de que la persona investigada por un delito público doloso se niegue a colaborar voluntariamente en la recogida de sus datos biométricos y genéticos a efectos de su registro, el órgano jurisdiccional competente está obligado a autorizar una medida de recogida forzosa, sin poder apreciar si existen motivos fundados para presumir que el interesado ha cometido una infracción penal por la que es investigado, siempre que el Derecho nacional garantice posteriormente el control jurisdiccional efectivo de las condiciones de esa investigación, de la que deriva la autorización para la recogida”.

Concluye el Tribunal que la Directiva se opone a la normativa nacional en la medida en que la autoridad competente no está obligada a comprobar y demostrar que la recogida de datos es estrictamente necesaria para cumplir los objetivos, así como si estos objetivos no pueden lograrse por medio de otras medidas menos invasivas. La calificación de “delito público doloso”, que permite la obtención de los citados datos, es demasiado genérica, pudiendo aplicarse esta disposición a prácticamente cualquier delito, independientemente de su gravedad o circunstancias concretas, lo que desvirtúa el requisito de necesidad estricta.

Está claro que LVA no realiza una recogida sistemática de datos personales dado que se limita a uno en particular, si bien es cierto, que el resto de datos del entrevistado obran en poder del responsable y del encargado del tratamiento y no resultaría difícil ponerlos en relación evidentemente. Pero en puridad, LVA sólo

accede exclusivamente a un dato, que, si bien es biométrico, sólo con un contraste de una base de datos donde se identifique a la persona tendría esa capacidad. Es decir, una voz anonimizada, es decir ciega, que no esté en relación con ningún otro dato, podría llevar a la identificación de una persona, pero resultaría cuando menos complicado. En este caso es el encargado del tratamiento quien tiene la posibilidad de identificar a la persona con la voz, no necesariamente la herramienta LVA, que como tal sólo analiza los parámetros de la misma en los términos descritos en las características de la herramienta.

Pero, aunque LVA accediera al resto de datos personales, con el cumplimiento de las garantías legales, estaríamos ante un uso proporcional de datos biométricos que requeriría, evidentemente, las máximas medidas de tratamiento y protección de los mismos.

IV. *Layered Voice Analysis*. La IA en la entrevista laboral

Siguiendo la clasificación del Reglamento sobre el uso de la IA, la herramienta que nos ocupa podría situarse en dos niveles de riesgo:

- Por una parte, se puede encuadrar en un **nivel de alto riesgo**, en la medida en que su principal dato es la voz, considerado dato biométrico. El citado reglamento considera de alto riesgo todo sistema que trabaje con datos biométricos, sujetándolo a requisitos estrictos.
- Por otra, un **nivel de riesgo medio**, que engloba los sistemas de interacción persona – máquina, en los que ésta última está entrenada para detectar emociones. El prestador del servicio debe asegurar ciertos mínimos en cuanto a transparencia e información al usuario.

El objetivo de la LVA es detectar los casos en que existe una intención real de engaño por parte del candidato, midiendo ciertos parámetros del estado psicofísico de éste, como puedan ser el estrés emocional, cognitivo, ocultamiento

de información, cambios en la voz... está basada en modelos matemáticos y datos obtenido de muestras de voz, que analiza buscando variaciones en intensidad y frecuencia.

Como se ha indicado, la inteligencia predictiva puede ser usada para analizar datos biométricos como, por ejemplo, la voz. Una aplicación de esta técnica puede orientarse al trabajo en Recursos Humanos y selección de personal. Para aplicar el análisis de voz a entrevistas de trabajo, hay que tener en cuenta varios aspectos:

La primera premisa básica es que en las entrevistas de trabajo no se pueden realizar preguntas sobre cuestiones personales que no afecten al desempeño del trabajo (derecho a la intimidad). Cabe recordar que prácticamente cualquier estado tiene en sus textos constitucionales, cartas magnas, etc., reconocido entre el catálogo de derechos fundamentales el equivalente al derecho a la intimidad del art. 18 de la CE.

Para que estas prácticas de selección sean lícitas debe existir una estrecha relación entre las investigaciones en forma de preguntas realizadas por el empresario, el contenido de la tarea y la capacidad requerida para hacer esa tarea²⁴. Es decir, se permite el acceso a la información reservada del candidato cuando tal requisito sea esencial para el normal desarrollo de las tareas, pero no estaría permitido investigar

²⁴Sin ir más lejos STSJ M 8378/2020, de 20 de setiembre, reconoce sobre la entrevista personal, que esta Sala -contencioso- *ha destacado su idoneidad como elemento de contraste (sentencia de 3 de febrero de 2020, recurso 135/2017, con cita de otras como la de 31 de marzo de 2017, recurso 945/2015), pues permite abordar aspectos no detectables en otras pruebas y constituye un sistema plenamente aceptado y asumido, con el fin de verificar la adecuación de la persona participante para el ejercicio de las funciones propias de la categoría de Policía. Sin embargo, la misma sentencia no duda en reconocer que no es posible validar la entrevista cuando ésta se centra en cuestiones ajenas al contenido propio de la entrevista y los factores cuya valoración deben presidirla, adentrándose en ocasiones, en aspectos de la formación y experiencia profesional del opositor, ajenos a su objeto, sin que tampoco se justifique el por qué tales cuestiones son evaluadas negativamente.* En idénticos o parecidos términos se manifiesta la STSJ M 279/2021, de 12 de febrero, del mismo órgano. Igualmente sírvase ver STS 1165/2022, de 31 de marzo, que desestima el recurso de casación interpuesto por la Abogacía del Estado frente a la última sentencia meritada, confirmando así el criterio de la Sala de lo Contencioso-administrativo del TSJ de Madrid.

todo lo que no sea relevante para determinar la aptitud del candidato respecto del puesto. Se entiende entonces que no estarían permitidas las investigaciones dirigidas a establecer de manera preventiva si el trabajador es diligente, honesto, serio, trabajador, tolerante... porque no son cualidades inherentes a ninguna tarea, sino a la figura moral de todo trabajador. Tampoco serían adecuadas preguntas sobre el uso de drogas, alcohol o participación en apuestas, en cuanto afectan al derecho a la intimidad del candidato.

Sí existen y están permitidas determinadas prácticas que permiten conocer la personalidad, habilidades y aptitudes del candidato en aras a decidir si es adecuado para el puesto de trabajo. Pero siempre deben 1) respetar los límites de respeto a su dignidad, intimidad y, en definitiva, privacidad, 2) no tener en cuenta factores establecidos como prohibidos para realizar un trato desigual, por ser discriminatorio, y 3) contar con el consentimiento del candidato. (Aspecto este último bastante controvertido en tanto que es evidente el desequilibrio de poderes de las partes de la relación laboral y la posición de subordinación de la persona trabajadora respecto del empleador).

Ahora bien, realizar este proceso de reclutamiento o promoción, con la misma finalidad, pero utilizando sistemas de IA añade nuevos límites a esta fase de selección del personal por las potencialidades y peligros que entraña esta tecnología. La tecnología objeto de este informe no es exactamente una tecnología basada en IA, en el sentido que LVA no adopta la decisión de seleccionar o no, ni de proponer, ni de excluir impidiendo continuar con el proceso de selección, sino predominantemente en algoritmos que analizan la voz, mostrando una serie de características que se denotan por la misma. Sin embargo, los algoritmos ya se están empleando en pruebas de selección gamificadas que incluyen preguntas, rompecabezas u otros desafíos para realizar evaluaciones predictivas sobre un candidato o para medir sus características, como la destreza, el tiempo de reacción

u otras capacidades. Estas evaluaciones gamificadas, también conocidas como evaluaciones psicométricas, se están convirtiendo en una herramienta de reclutamiento cada vez más común, se utilizan junto con las soluciones de pruebas psicométricas tradicionales o como alternativa a ellas para el proceso de contratación o de selección de personal. Pero se deben tener muy en cuenta sus riesgos.

Entonces, habría dos tipos de limitaciones en razón a dos ámbitos de incidencia en la persona: por un lado, la intimidad del candidato en cuanto al contenido de las preguntas, por otro, la dignidad, en cuanto a la metodología utilizada (tecnología IA) [amén de todas las garantías aplicables en tanto que hablamos de tratamiento de datos personales]. Y todo ello, bajo la limitación general de no discriminación.

Sí parece claro que estamos ante datos biométricos, y cuanto mayor es la sofisticación del sistema de datos biométricos, mayor serán los problemas para el juicio de validez del control articulado empresarialmente sobre ellos por resultar más invasivos. Es decir, a más difusa, sutil u oculta resulte la información real captada tras los correspondientes procesamientos de datos cruzados, mayor sospecha sobre su ilegitimidad porque más indefensión genera, dificultando o impidiendo ejercer derecho alguno hasta que no se produzca la actualización del riesgo en un daño personal.

Por último, ante una posible colisión entre los derechos de la persona trabajadora y el derecho a la libertad de empresa del empleador (y los poderes de organización, gestión y control que de él emanan) habría que acudir a la **ponderación de los derechos en juego** para determinar cuando está o no permitido realizar una práctica empresarial concreta para tomar decisiones sobre la gestión laboral. Es decir, hay un conflicto entre el interés del empresario a conocer preventivamente las capacidades de un candidato y el derecho del candidato a no sufrir penetrantes intromisiones en la esfera de su vida privada.

Por otro lado, hay que considerar la igualdad de oportunidades y no discriminación como limitación principal a la voluntad del empleador, tanto en los procesos de contratación como de promoción y ascenso. Cualquier entrevista de trabajo que se realice como prueba personal para acceder a un puesto debe estar presidida por el principio de igualdad en el acceso al empleo, no pudiendo establecerse discriminación alguna, directa o indirecta, basada en motivos de origen, racial o étnico, sexo, edad, estado civil, religión o convicciones, opinión política, orientación sexual, afiliación sindical, condición social, lengua dentro del Estado, salud y discapacidad. (art.5 y 39 Ley empleo / Art. 4.2.c y e ET).

Como ya se ha señalado, lo ideal sería evitar cualquier pregunta sobre cuestiones personales que no afecten al desempeño en el puesto de trabajo. Sin embargo, con la finalidad de concretar la idoneidad del candidato en el ámbito de la exploración psicológica, las **pruebas psicotécnicas y los test de personalidad** se utilizan habitualmente en estos procesos de selección para tratar de averiguar el carácter o la personalidad del candidato en relación con el puesto de trabajo que se trata de cubrir. Es decir, directamente no son preguntas de conocimientos sobre el objeto del puesto de trabajo, pero tratan de conocer otros aspectos fundamentales de la persona que les permita predecir su desempeño futuro en la empresa.

Diferenciamos tres tipos:

- i. Los **test psicotécnicos** son pruebas estandarizadas, que sirven para medir conductas, capacidades y habilidades de un candidato o candidata de cara a una posible contratación. En esta categoría se incluyen los test de inteligencia y los test de aptitudes
- ii. Los **test de personalidad** tratan de identificar los principales rasgos que definen las emociones, los pensamientos, las conductas y las formas de adaptación de la persona candidata.

- iii. Los **test proyectivos** tratan de recabar datos sobre la forma de procesar la información a través de estímulos que pretenden llegar al subconsciente de las personas.

En principio, las partes están obligadas a actuar de buena fe, por lo que el empresario tiene derecho a incluir cuantas preguntas estime oportunas, siempre que guarden relación con las aptitudes profesionales necesarias para el puesto de trabajo, y el candidato estará obligado a responder correctamente.

Ahora bien, para que se admitan estas prácticas, deberían darse las siguientes condiciones de admisibilidad: 1) comunicar al candidato las cualidades psicofísicas necesarias para realizar el trabajo, 2) comunicar los tipos de test que se van a realizar y 3) no sobrepasar los límites de aptitud requeridos para la prestación del trabajo. Solo así estará dando su consentimiento informado y no se vulnerará su intimidad. (Cuando estas pruebas tengan un contenido clínico, es decir, que se acerque demasiado a identificar alguna patología o a conocer el estado psíquico de una persona, entonces solo podrán hacerse con el consentimiento del candidato y siempre realizados por un profesional.)

El **polígrafo** sería un caso extremo de procedimiento, ya que registra las variaciones físicas que se producen en el organismo de una persona en relación a su estado psicológico. Es decir, registra reacciones corporales ante preguntas para deducir de ellas conclusiones sobre la corrección subjetiva de aquello que se declara, por lo que supone una desvalorización de la declaración expresa y lesiona la intimidad del candidato.

Podría considerarse que la tecnología presentada se incluye en la tipología de estudio de la personalidad de los candidatos, pues a través de sus reacciones a las preguntas, más que del propio contenido de las respuestas, la aplicación puede detectar, medir, clasificar y, en definitiva, perfilar, a la persona trabajadora con base

en los parámetros con los que haya sido programada para obtener los resultados deseados. Y claro, está obteniendo muchos datos del candidato que no solo se refieren a los conocimientos que pueda tener o no y que le capacitan para ese puesto de trabajo, sino también datos de su propia persona, objetivados, cuantificados y estandarizados. Pero también podría tratarse de tecnología muy similar a un polígrafo si consideramos que está obteniendo una información – biométrica, además – relacionada con las reacciones del candidato cuando responde y no con el contenido de su respuesta. (Y mejor que yo, sabrás tú que los datos biométricos son una categoría de datos personales de especial protección).

Por todo lo anterior, es complicado encajar los peligros del uso de esta aplicación en cuanto a posible vulneración del derecho a la igualdad, en tanto que no se tomen ninguno de los factores expresamente incluidos en las disposiciones legales, tales como sexo, edad, religión...

Quizá, entonces, sería más correcto advertir de los peligros de esta tecnología por posibles intromisiones ilegítimas en la esfera personal de la persona trabajadora, en su intimidad y dignidad, dada la cantidad y la profundidad de los datos que se pueden extraer sobre sus reacciones y, sobre todo, las decisiones que se van a tomar en consecuencia. Es decir, nos encontraríamos ya, no en el terreno de la igualdad del artículo 14 CE, sino en la dignidad (10.1 CE) y en la intimidad (18.1 CE).

Y como todo ello se realiza a través de medios tecnológicos y digitales, también cabría atender a los artículos 87-91 LOPD (derechos digitales laborales) y su expreso reconocimiento en el artículo 20.bis ET. Y, si fuera una norma vigente (que, además, parece que no va a salir nunca y si sale no será con el contenido del borrador que todos tenemos), también habría de tenerse en cuenta, la propuesta

de Ley de Inteligencia artificial de la UE que, sin duda, calificaría esta práctica como de alto riesgo²⁵, con lo que ello conlleva.

Cuando se incluyan categorías especiales de datos personales, solo se permitirá el recurso a estos sistemas en virtud de las condiciones acumulativas establecidas en el art. 22.4 RGPD, salvo que se aplique el artículo 9.2, a) o g) RGPD, y que se hayan tomado de medidas adecuadas para salvaguardar los derechos y libertades e intereses legítimos, en este caso, del candidato.

El juicio de ponderación.

Estaríamos ante un conflicto de intereses entre el interés del empresario de conocer al trabajador para conocer también preventivamente las capacidades profesionales reales de éste, para poder insertarlo en el puesto justo de la organización empresarial, y el derecho del trabajador para no sufrir penetrantes intromisiones a la esfera de su vida privada y a no ser sometido a peligrosas comprobaciones y juicios sobre cualidades propias e intrínsecas no referentes a los aspectos objetivos de la relación de trabajo.

El juicio de idoneidad exige que la restricción al derecho fundamental de que se trate permita alcanzar efectivamente un fin legítimo, como es la toma de decisiones sobre la organización de la empresa y la gestión del personal. De acuerdo con el juicio de necesidad, la medida o restricción del derecho fundamental debe ser indispensable para lograr el fin legítimo, no existiendo una alternativa más benigna con el derecho fundamental en cuestión.

²⁵Artículo 6.2 en relación al Anexo III, al considerarse como alto riesgo sistemas de IA destinados a utilizarse para la contratación o selección de personas físicas, especialmente para anunciar puestos vacantes, clasificar y filtrar solicitudes o evaluar a candidatos en el transcurso de entrevistas o pruebas.

Respecto al juicio de proporcionalidad en sentido estricto, aplicable sólo si la restricción es considerada idónea y necesaria, este determinará como válida una práctica cuando, para el logro de una finalidad legítima se requiera indispensablemente la restricción de otro derecho fundamental de modo tal que la satisfacción de uno sólo puede realizarse a costa del otro.

El *Dictamen 2/2017 sobre el tratamiento de datos en el trabajo* del GT 29²⁶ recoge que independientemente de la base jurídica del tratamiento de datos que haya la empresa, antes de su inicio se debe realizar una prueba de proporcionalidad con el fin de determinar si el tratamiento es necesario para lograr un fin legítimo, así como las medidas que deben adoptarse para garantizar que las violaciones de derechos de la vida privada se limiten al mínimo.

Claro, lo que ocurre es que todo este esquema se aplicaría en caso de judicialización de una práctica empresarial por posible vulneración de derechos fundamentales de la persona trabajadora. Mientras tanto, es un juicio preventivo que debería hacer la empresa a la hora de implementar su tecnología, pero nada más...

Por último, la aplicación del artículo 24 CE, el **derecho a no declarar contra sí mismo, a no confesarse culpable o a la presunción de inocencia**, solo parece tener cabida en el ámbito laboral en el contexto de un procedimiento de investigación interna en la empresa, pero, en principio, no encontraría su encaje en la situación que estás trabajando, sino más bien todos los otros derechos anteriormente mencionados.

Sí podría ser interesante tener en cuenta las **consecuencias de una mentira** en el marco de una relación laboral contractual (válido para los procesos de promoción,

²⁶Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. Disponible en wp251rev.en.aepd.es

en tanto que hay relación laboral viva, pero no en los de reclutamiento). ¿Qué pasaría si el candidato miente en las preguntas? ¿Y si no miente en el contenido de las respuestas, pero su comportamiento y reacción es interpretado como incorrecto o erróneo? ¿Podría reaccionar la empresa al respecto con una sanción?

En principio, mentir sería una transgresión de la buena fe contractual (art. 20 ET) que funcionaría como causa justificativa de un despido disciplinario (art. 54 ET). Pero, en Francia por ejemplo, la jurisprudencia considera esa mentira como legítima y no lo considera dolo, porque el candidato no está obligado a responder a nada que no guarde relación con el desempeño del puesto, por lo que sería una forma útil de garantizar el respeto a su vida privada y de impedir al empresario acceder a información sobre aspecto que no tiene derecho conocer.

En definitiva, asumiendo el carácter invasivo o intrusivo de los sistemas basados en la biometría, la regla debe ser adoptar un sistema alternativo menos incisivo en los derechos fundamentales. Es decir, excluir el método basado en un reconocimiento biométrico como primera opción y primando otros métodos menos invasivos (garantía de proporcionalidad), introduciendo aquel otro solo si es estrictamente necesario (justificación reforzada) y previa evaluación del impacto sobre eventuales riesgos para derechos fundamentales (garantía de procedimiento), en este caso, de las personas candidatas a un puesto de trabajo.

Sería inoperante, como regla general, la base jurídica del consentimiento (no exactamente libre) del trabajador, mientras que la necesidad de ejecución contractual o de satisfacer un interés legítimo empresarial tendrían importantes obstáculos por la interpretación estricta de la necesidad contractual y el severo juicio de ponderación que se precisa para conceder prioridad al interés legítimo, cuyo predominio queda en duda por el fuerte impacto que estos tratamientos producen en la esfera jurídica de los trabajadores.

A mayor abundamiento, el tratamiento de datos personales en el ámbito laboral ha sido objeto de estudio y análisis detallado por parte de la AEPD, por lo que resulta recomendable seguir, en el ámbito de la UE, sus indicaciones al respecto²⁷.

V. Protección de Datos

El artículo 9 RGPD señala la prohibición del tratamiento de aquellos datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, **datos biométricos dirigidos a identificar de manera unívoca a una persona física**, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

Obviamente a lo largo del presente informe se ha recalcado que la voz tiene consideración de dato biométrico, luego le resultará de aplicación lo dispuesto en el esta disposición. Más, si cabe, cuando todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, conforme dispone el art. 22.1 RGPD.

Evidentemente tanto el art. 9 como el 22 del RGPD cuentan con excepciones a esa regulación general prohibitiva. Básicamente el consentimiento del interesado, expresado de forma explícita para el tratamiento de dichos datos personales - biométricos-, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición no puede ser levantada por el interesado; ampara el tratamiento de este tipo de datos.

²⁷FAQS sobre tratamiento de datos personales en entorno de trabajo de la AEPD, consultar en <https://www.aepd.es/es/preguntas-frecuentes/3-tratamiento-de-datos-en-el-ambito-laboral>

Como ya hemos señalado, el caso particular de LVA estaría situado en el nivel de RIESGO ALTO y en el de RIESGO LIMITADO, correspondiendo, por tanto, aplicar los niveles de control específicos. En particular, los propios del RGPD. Así a excepción basada en el consentimiento explícito del interesado, que permite el tratamiento de datos biométricos, no exime al responsable del tratamiento de adoptar “las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión”.

Por tanto, en este punto, lo importante en este caso no es el consentimiento, ni la ausencia de alternativa a la facilitación de datos, algo que también ocurriría en el caso de la herramienta LVA, toda vez que una entrevista personal no aportaría la misma información que la que genera la herramienta. Aquí lo verdaderamente importante es que es **ABSOLUTAMENTE IMPRESCINDIBLE**, además reseñamos especialmente que aplica a todo el ámbito de la Unión Europea la **EVALUACIÓN DE IMPACTO PREVIA A LA ACTIVIDAD**.

Consecuentemente también habrá que desarrollar una **ACTIVIDAD DE TRATAMIENTO ESPECÍFICA** para ese supuesto concreto.

Está claro que es de todo punto necesario justificar debidamente el motivo del uso de la herramienta dejando de forma totalmente clara y determina el porqué de la necesidad de la herramienta, diferenciándola de una entrevista personal (que no comportaría tratamiento de datos biométricos -siempre que no se grabara la misma-).

Para introducir, con estricto cumplimiento legal la herramienta LVA, deberá realizarse con carácter previo un juicio de proporcionalidad, valorando la idoneidad de la medida y la necesidad del tratamiento. Además, debe llevarse a cabo una

Evaluación de Impacto en relación a los requisitos marcados por el art. 35 del RGPD²⁸.

El propio texto legal determina cuales son las características que debe respetar la evaluación, que deberá incluir como mínimo:

- a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
- b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- c) una evaluación de los riesgos para los derechos y libertades de los interesados, y
- d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

La Evaluación de Impacto en la Protección de Datos Personales es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los

²⁸La evaluación de impacto relativa a la protección de datos se llevará a cabo, conforme el art. 35 RGPD, regulación que básicamente se reproduce en las regulaciones de carácter internacional, incluyendo la de la República Popular China, de forma sistemática y exhaustiva cuando se afecte a aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar, lo que entraría dentro de las características de la herramienta LVA.

que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos.

El análisis de riesgos para un determinado tratamiento va a permitir identificar los riesgos que amenazan los datos de los interesados y así poder establecer una respuesta individualizada al nivel de riesgo existente adoptando las salvaguardas necesarias para reducirlos hasta alcanzar el objetivo de un **nivel de riesgo aceptable**.

Tal y como prevé la normativa, las Evaluaciones de Impacto se deben de llevar a cabo con antelación al inicio de tratamiento en aquellos casos en los que sea más probable que exista un alto riesgo para los derechos y libertades de los afectados, en el resto puede llevarse a cabo con el tratamiento ya iniciado, pero es importante evitar la plasmación del riesgo en daños concretos para los datos personales de los interesados al objeto de evitar sanciones.

En la evaluación de impacto (EIPD), además, debe tenerse en consideración el contexto en el que la misma se ha de llevar a cabo. A estos efectos será necesario:

- Describir el ciclo de vida de los datos: Descripción detallada del ciclo de vida y del flujo de datos en el tratamiento. Identificación de los datos tratados, intervinientes, terceros, sistemas implicados y cualquier elemento relevante que participe en la actividad de tratamiento.
- Analizar la necesidad y proporcionalidad del tratamiento: Análisis de la base de legitimación, la finalidad y la necesidad y proporcionalidad del tratamiento que se pretenden llevar a cabo.

En cuanto hace referencia a la gestión de riesgos, he hace preciso:

- Identificar amenazas y riesgos: Identificación de las amenazas y riesgos potenciales a los que están expuestos las actividades de tratamiento.

- Evaluar los riesgos: Evaluación de la probabilidad y el impacto de que se materialicen los riesgos a los que está expuesta la organización.
- Tratar los riesgos: Respuesta ante los riesgos identificados con el objetivo de minimizar la probabilidad y el impacto de que estos se materialicen hasta un nivel de riesgo aceptable que permita garantizar los derechos y libertades de las personas físicas.

Finalmente la EIPD finalizará con la conclusión y validación, que se manifiestan en el Plan de acción y conclusiones. Este documento contendrá necesariamente un informe de conclusiones de la EIPD donde se documente el resultado obtenido junto con el plan de acción que incluya las medidas de control a implantar para gestionar los riesgos identificados y poder garantizar los derechos y libertades de las personas físicas y, si procede, el resultado de la consulta previa a la autoridad de control a la que se refiere el artículo 36 del RGPD.

Adicionalmente a las fases que componen una EIPD, es recomendable que exista un proceso de supervisión y revisión de la implantación o puesta en marcha del nuevo tratamiento con el objetivo de garantizar la implantación de las medidas de control descritas en el Plan de acción.

La EIPD no puede entenderse como un protocolo inerte, al contrario, debe concebirse como un proceso de mejora continua, de forma que esta se revise siempre que se modifique o actualice cualquier aspecto relevante de las actividades de tratamiento.

La adaptación y adecuación continua ante cambios en la descripción del tratamiento o en la experiencia que muestre amenazas o riesgos desconocidos hasta entonces (los fines y medios), exigirá la realización de una nueva evaluación de impacto, lo que implica la necesidad de generar un nuevo informe y un plan de acción con las nuevas medidas de control que se hayan incluido en la misma.

Por el contrario, cuando los cambios sobre el tratamiento no resulten significativos, porque no suponen el advenimiento de nuevas amenazas ni riesgos sobre los derechos y libertades de los interesados, simplemente se llevará a cabo una valoración de los cambios producidos, documentando de forma clara la no necesidad de implantar nuevas medidas de control adicionales.

En todo caso, a los efectos de elaborar la EIPD, recomendamos seguir las instrucciones, así como emplear la herramienta de evaluación de impacto de la AEPD²⁹.

VI. Conclusiones

La tecnología LVA usa conjuntamente cuestionarios específicos con análisis avanzado de voz para evaluar la fiabilidad de las respuestas de un candidato. Su uso preferente es en el área de Recursos Humanos, tanto en la selección de empleados como en el seguimiento posterior.

Debido al riesgo que entraña el tratamiento de estos datos, previo a su puesta en marcha es imperativo recabar el consentimiento expreso e informado del usuario sobre los objetivos del uso de este sistema, las garantías de seguridad que ofrece y la forma de custodia de los datos obtenidos. Es en este punto cuando pueden producirse discriminación en el acceso al empleo, en caso de que el candidato no consienta al tratamiento de sus datos.

El LVA se presenta como una herramienta objetiva y justa, capaz de evaluar a los candidatos de manera imparcial y precisa. Sin embargo, la realidad es que la programación de estos algoritmos se basa en datos obtenidos a partir de la

²⁹<https://www.aepd.es/es/documento/guia-evaluaciones-de-impacto-rgpd.pdf>

observación y el análisis de la conducta de las personas en situaciones de nerviosismo y estrés, como pueden ser las entrevistas laborales.

Esto plantea la duda de si las respuestas físicas valoradas por estos sistemas se deben realmente a que el candidato esté mintiendo o si son el resultado del propio contexto de tensión y ansiedad de la entrevista laboral. Además, existe el riesgo de que los algoritmos incorporen sesgos y discriminaciones, ya sea por el tipo de datos utilizados para su entrenamiento o por la propia programación de los mismos.

Por lo tanto, es importante tener en cuenta que la aplicación de la inteligencia artificial en la evaluación de candidatos para un puesto de trabajo debe ser cuidadosamente analizada y regulada, de manera que se evite cualquier tipo de discriminación y se respeten los derechos fundamentales de los candidatos, incluyendo su derecho a la privacidad y a la no discriminación.

El uso de este sistema debe estar sujeto a las directrices europeas, o de cualquier otra normativa que resulte de aplicación, en materia de protección de datos, al considerarse la voz un dato biométrico, como ya se ha indicado, limitándose su uso a los fines especificados y evitando su tratamiento fuera de los objetivos de selección o seguimiento planteados por la empresa.

También conviene destacar que hay que analizar detenidamente las preguntas que, desde la perspectiva de la garantía y salvaguarda de la intimidad y de los derechos fundamentales que asisten a los sujetos que van a ser objeto de análisis por LVA, se les pueden formular, para evitar infringir las normas básicas, que harían nula cualquier decisión adoptada a posteriori y que, a su vez, supondría la aplicación estricta de las prohibiciones de tratamiento de datos personales biométricos -voz- en este caso.

Por lo tanto, desde una perspectiva jurídica los límites de la legislación laboral, en consonancia con los derechos fundamentales, junto con la privacidad amparada por la normativa de protección de datos, incluso, allí donde existe, la propia reguladora de la IA, son todos ellos parámetros que directamente inciden en el uso de la herramienta LVA. Así visto, es de todo punto imprescindible analizar caso por caso para cada Estado donde se prevea su aplicación analizar todas estas cuestiones, partiendo del hecho cierto de que la normativa de derechos fundamentales es similar en todos ellos, sirva de ejemplo la propia constitución iraquí, siendo la propia de la privacidad la que, aún con patrones comunes, presenta matices más diferenciadores.

Sin perjuicio de mejor opinión fundada en derecho

Salamanca, 24 de mayo de 2023

VII. Bibliografía de referencia

- Alameda Castillo, M. T. (2021) "Reclutamiento tecnológico. Sobre algoritmos y acceso al empleo", *Revista Temas Laborales*, N° 159, 2021, págs. 11-52.
- Baz Rodríguez, J (2021) *Los nuevos derechos digitales laborales de las personas trabajadoras en España: vigilancia tecnificada, teletrabajo, inteligencia artificial*, Big Data. CISS
- Baz Tejedor, J. A. (2021) *Inteligencia artificial y privacidad del trabajador predecible*. En Baz Rodríguez, J (2021) *Los nuevos derechos digitales laborales de las personas trabajadoras en España: vigilancia tecnificada, teletrabajo, inteligencia artificial*, Big Data. CISS
- Comité Europeo de Protección de Datos & Supervisor Europeo de Protección de datos (2021) 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. Disponible en:
[EDPB-EDPS Joint opinion 202105 AI Regulation ES_np.docx \(europa.eu\)](#)
- Fernández, C. (2023) China prepara una regulación para la Inteligencia Artificial Generativa. Diario La Ley, nº 72, Sección Ciberderecho. Disponible en: [diariolaley - Documento \(laleynext.es\)](#)
- Goñi Sein, J.L. & Palomeque López, M. C. (1988). *El respeto a la esfera privada del trabajador: un estudio sobre los límites del poder de control empresarial*. Civitas.
- Mercader Uguina, J. R. (2021) *Datos biométricos en los centros de trabajo*. En Baz Rodríguez, J (2021) *Los nuevos derechos digitales laborales de las personas trabajadoras en España: vigilancia tecnificada, teletrabajo, inteligencia artificial*, Big Data. CISS.

- Mercader Uguina, J. R. (2022) *Algoritmos e inteligencia artificial en el derecho digital del trabajo*, Tirant lo Blanch.
- Molina Navarrete (2021). *Datos y derechos digitales de las personas trabajadoras en tiempos de (pos)covid19: entre eficiencia de gestión y garantías*, Cristóbal Molina Navarrete, 2021. Bomarzo.
- Peralta, L.A. (2023) ¿Es realmente necesaria una regulación de la inteligencia artificial? Cinco Días. Disponible en: [cincodias.es/pais.com](https://www.cincodias.es/pais/comunicacion/2023/05/02/ia-regulacion-2023-05-02.html)
- Rivas, P. (2021) Geolocalizar a los trabajadores no es invasión de su intimidad si el dispositivo utilizado para ello es propiedad de la empresa. Revista de Jurisprudencia Laboral, nº 3/2021. Disponible en [BOE.es](https://www.boe.es/boe-diccionario-sinonimos/ver-boe/BOE-A-2021-10000)
- Vough, R. T. (2019) Memorandum For The Heads Of Executive Departments And Agencies on "Guidance for Regulation of Artificial Intelligence Applications". Disponible en:
- Zorraquino, A. (2021) Resumimos la propuesta europea de Reglamento sobre los usos de la Inteligencia Artificial. Preiscopio Fiscal y Legal. Disponible en: [Reglamento Inteligencia Artificial \(pwc.es\)](https://www.pwc.es/preiscopio/2021/05/resumimos-la-propuesta-europea-de-reglamento-sobre-los-usos-de-la-inteligencia-artificial/)