Diputació de València | Protecció de Dades i Seguretat de la Informació

DivalData

Boletín extraordinario con motivo del día Europeo de la Protección de Datos

Boletín extraordinario 2025

PRINCIPALES CUESTIONES RELATIVAS A LA APLICACIÓN DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL POR LA ADMINISTRACIÓN PÚBLICA

ÍNDICE

PRINCIPALES CUESTIONES RELATIVAS A LA APLICACIÓN DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL POR LA ADMINISTRACIÓN PÚBLICA

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos cuadernos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Cuaderno accede al siguiente enlace.

"En el día de la protección de datos de carácter personal es necesario hacer hincapié, una vez más, en el deber que la Administración pública tiene en la adopción de medidas jurídicas, organizativas y técnicas para salvaguardar el derecho fundamental a la protección de datos de carácter personal".

INTRODUCCIÓN

Cada día son más las Administraciones públicas las que buscan la aplicación de la Inteligencia Artificial (en adelante, IA) A a fin de lograr, entre otros, la mejora en la personalización, eficiencia, efectividad, equidad y transparencia de los servicios públicos. La IA está revolucionando la relación entre las administraciones públicas y la ciudadanía, marcando un antes y un después en la prestación de servicios públicos.

Huelga decir, que la IA, lejos de una perspectiva alarmista y detractora, puede aportar un sinfín de ventajas o beneficios para nuestra sociedad. No cabe duda, que la regulación por Ley y la aplicación de la ética, son necesarias. Pero, sin entrar en el debate de esto último, a través del presente, se aporta una relación de usos o fines de la IA en el ámbito de la Administración pública, así como una relación de ejemplos de dicho uso en la Administración Local.

Por otro lado, a fecha del presente Boletín, nos encontramos en los albores de la aplicación del vigente Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante, Reglamento de Inteligencia Artificial o RIA).

En anterior publicación extraordinaria, ya hicimos un adentramiento en qué suponía el incipiente uso de la IA, en particular, a nivel del sector público. A partir de los borradores del texto, que estaba elaborándose a nivel de Unión Europea, se desgajaron las disposiciones más relevantes, pero sin conocer cuál sería la articulación final de las mismas.

Ahora, publicada en el D.O.E. la versión vigente del Reglamento, nos ocupamos, en esta publicación, de aportar las principales cuestiones, de carácter jurídico, a tener presente a los efectos de crear, implementar y/o distribuir IA por parte de la Administración pública.

"El nuevo prestador tendría base de legitimación para tratar los datos personales en la medida en que sean estrictamente necesarios para la gestión del servicio público de suministro de abastecimiento de agua en red secundaria, siempre respetando el resto de los principios recogidos en el RGPD".

Por último, en este boletín, extraordinario por estar siempre asociado al Día Europeo de la Protección de Datos, se ha tratado de mostrar la especial sujeción del uso de la IA a la legislación en protección de datos de carácter personal. Es por esto que, con arreglo a cuanto ya anticipo la Agencia Española de Protección de Datos, entendemos oportuno, extractar la parte más significativa de aquello que nos dijo la autoridad de control estatal.

1. UTILIZACIÓN DE LA IA EN LA AA.PP. LOCAL

1.1. Listado de usos, agrupados por fines

La inteligencia artificial (de ahora en adelante, IA) está transformando diversos sectores a nivel global, y la administración pública no es la excepción. Los ayuntamientos, como órganos de gestión local, se están adaptando a las nuevas tecnologías para mejorar la eficiencia de sus servicios, optimizar la toma de decisiones y ofrecer una atención más personalizada a los ciudadanos. En este contexto, varios gobiernos locales han comenzado a implementar, o tienen planes para hacerlo en el futuro cercano, sistemas basados en IA. Estos sistemas pueden abarcar desde la automatización de trámites administrativos hasta la predicción de necesidades urbanísticas o la gestión inteligente del tráfico. Este fenómeno no solo implica un avance en términos tecnológicos, sino que también abre un abanico de posibilidades para transformar la relación entre las autoridades locales y los ciudadanos, haciendo que los servicios públicos sean más rápidos, accesibles y adaptados a las necesidades de la comunidad. En este sentido, es importante examinar ejemplos concretos de cómo algunos ayuntamientos están adoptando la IA para entender mejor su impacto y potencial.

La IA está revolucionando la relación entre las administraciones públicas y la ciudadanía, marcando un antes y un después en la prestación de servicios públicos. Este poder transformador se manifiesta en la capacidad de la IA para redefinir dinámicas tradicionales, introduciendo niveles sin precedentes de eficiencia,

"La IA está revolucionando la relación entre las administraciones públicas y la ciudadanía, marcando un antes y un después en la prestación de servicios públicos. Este poder transformador se manifiesta en la capacidad de la IA para redefinir dinámicas tradicionales, introduciendo niveles sin precedentes de eficiencia, personalización y capacidad de anticipación en la prestación de servicios públicos".

personalización y capacidad de anticipación en la prestación de servicios públicos.

En este contexto, y tal como define Pedro Padilla Ruiz en su articulo sobre *"Aplicaciones de la inteligencia artificial en los Ayuntamientos"* se pueden identificar dos grandes áreas de aplicación de la IA en el ámbito público:

- **Sistemas para la ejecución de actos administrativos**

En este ámbito, la IA se utiliza para automatizar decisiones y ejecutar acciones previamente reservadas a la intervención directa de las personas. Los sistemas inteligentes pueden analizar datos, evaluar escenarios y llevar a cabo tareas de manera autónoma, lo que significa que procesos antes manuales y laboriosos ahora pueden realizarse con mayor rapidez. Por ejemplo, la expedición de licencias, la validación de documentos o la asignación de recursos son actividades que la IA puede gestionar con alta eficiencia. Este nivel de automatización libera a los funcionarios de tareas repetitivas, permitiéndoles enfocarse en cuestiones estratégicas y en la resolución de problemas complejos. La capacidad de la IA para agilizar trámites y procesos administrativos no solo mejora los tiempos de respuesta, sino que también garantiza una mayor precisión en la toma de decisiones. Esto es crucial para evitar errores, reducir la burocracia y ofrecer a la ciudadanía servicios más consistentes.

- **Sistemas de apoyo a las actuaciones administrativas**

En este contexto, la IA se convierte en una herramienta de soporte clave para los procesos de toma de decisiones humanas. Estos sistemas analizan grandes volúmenes de datos y generan información útil que los responsables administrativos pueden utilizar para diseñar políticas más efectivas y adaptadas a las necesidades reales de la ciudad.

Una de las aplicaciones más destacadas es el análisis predictivo. A través de este enfoque, la IA permite a las administraciones anticiparse a problemas, prever demandas futuras y planificar recursos con mayor precisión. Por ejemplo, en situaciones de emergencia o durante el diseño de estrategias a largo plazo, la capacidad de anticipar desafíos y necesidades facilita una gestión preventiva y eficaz.

"Aunque la IA agiliza y mejora estos procesos no debemos olvidar que la responsabilidad y supervisión final deben recaer en el factor humano".

Esta tecnología también mejora la capacidad de respuesta de las administraciones frente a cambios repentinos en el entorno, como el crecimiento poblacional, crisis económica o desastres naturales.

Al evitar posibles obstáculos, las instituciones pueden adaptarse rápidamente, garantizando la continuidad y calidad de los servicios públicos.

Volviendo a la utilidad de la IA en la prestación de servicios públicos, podemos exponer algunos sectores que demuestran enormes mejoras en cuanto a la eficiencia, la transparencia y la calidad de los servicios municipales. Veamos algunos ejemplos:

1. Resolución de consultas sobre la ciudadanía

Los *chatbots* y asistentes virtuales basados en IA pueden proporcionar respuestas rápidas y precisas a las preguntas de la ciudadanía, mejorando la calidad de la atención y reduciendo la carga de trabajo de las personas empleadas.

Una de las mayores ventajas de la IA en el ámbito público es su capacidad para personalizar la interacción con los ciudadanos. Los asistentes virtuales y otros sistemas de IA pueden adaptar sus respuestas y servicios a las necesidades específicas de cada persona, ofreciendo una experiencia más satisfactoria.

Por ejemplo, un ciudadano que necesite información sobre impuestos locales puede recibir respuestas claras y adaptadas a su situación particular a través de un *chatbot*. Este tipo de interacción no solo simplifica la vida de los usuarios, sino que también mejora su percepción de la administración pública como una entidad accesible y centrada.

La personalización también fortalece el vínculo entre las instituciones y la ciudadanía, generando confianza y facilitando una comunicación más cercana y efectiva. Este enfoque centrado en el usuario contribuye a que las personas perciban a la administración como un aliado en lugar de un ente burocrático. Aunque la IA agiliza y mejora estos procesos no debemos olvidar que la responsabilidad y supervisión final deben recaer en el factor humano.

"Los algoritmos avanzados son capaces de analizar grandes cantidades de datos en tiempo real, identificando patrones, tendencias y áreas de mejora. Esto permite a las administraciones tomar decisiones basadas en información sólida y verificable, lo que a su vez incrementa la confianza pública en las instituciones".

2. Detección de fraudes y corrupción

En el sector público, una de las funciones que más se ha transformado con la irrupción de las nuevas tecnologías y la IA (especialmente, con minería de datos o *data mining)* ha sido la del control del cumplimiento normativo. Y, de entre todos los incumplimientos normativos, han sido el fraude y la corrupción los que posiblemente hayan merecido mayor atención.
La IA puede ayudar en la identificación de actividades fraudulentas y corruptas mediante el análisis de datos financieros y transaccionales. Esto es esencial para garantizar la integridad y la transparencia en el sector público.

En efecto, se han desarrollado un número significativo de sistemas informáticos antifraude y anticorrupción, empleados por los órganos inspectores y de control, destinados al análisis de grandes cantidades de datos para facilitar la detección de irregularidades y para orientar las subsiguientes actuaciones de gestión de riesgos o de inspección y sanción correspondientes.

3. Automatización de procesos y transparencia

La IA también desempeña un papel fundamental en la mejora de la transparencia y la eficiencia administrativa. Los algoritmos avanzados son capaces de analizar grandes cantidades de datos en tiempo real, identificando patrones, tendencias y áreas de mejora. Esto permite a las administraciones tomar decisiones basadas en información sólida y verificable, lo que a su vez incrementa la confianza pública en las instituciones.

Por ejemplo, la IA puede ser utilizada para monitorear la ejecución de presupuestos, identificar desviaciones en tiempo real y garantizar que los recursos se utilicen de manera eficiente. Asimismo, su capacidad para analizar datos históricos y actuales facilitar la identificación de problemas recurrentes y la implementación de soluciones.

Esta capacidad de análisis profundo no solo beneficia a las instituciones, sino que también refuerza su compromiso con la transparencia. Al disponer de estos datos de manera pública a la ciudadanía, las administraciones pueden demostrar su compromiso con una gestión responsable y accesible.

“La IA puede analizar grandes volúmenes de datos para identificar patrones y tendencias delictivas, ayudando a las fuerzas de seguridad a anticipar y prevenir actividades criminales”.

4. Refuerzo de la ciberseguridad

La IA se utiliza en la detección de amenazas cibernéticas y en la protección de infraestructuras críticas, lo que es fundamental en un mundo cada vez más digitalizado.

Nuestras administraciones reciben ataques informáticos cada día, de diverso tipo y de distinta gravedad. Con modelos de aprendizaje automático se pueden prevenir y limitar estos ataques. Como no podía ser de otra forma, la inteligencia artificial también está presente en la gestión informática y de la web municipal. Por ejemplo, el Ayuntamiento de Mataró predice y adapta la web oficial a las necesidades de los ciudadanos.

La inteligencia artificial se ha convertido en una herramienta imprescindible para garantizar la seguridad en un entorno digital en constante evolución. Su capacidad para detectar, prevenir y responder a amenazas cibernéticas, junto con su aplicación en la optimización de plataformas municipales, demuestra cómo esta tecnología está transformando la gestión pública, haciéndola más segura, eficiente y adaptada a las necesidades del siglo XXI.

5. Seguridad ciudadana

En este contexto, las administraciones locales tienen la posibilidad de desempeñar un papel significativo en su mejora mediante el uso de tecnologías de inteligencia artificial (IA). Estas herramientas no solo refuerzan la capacidad de prevención, sino que también optimizan los recursos.

Una de las aplicaciones más destacadas de la IA en este ámbito es la videovigilancia inteligente. Los sistemas de cámaras con IA, que pueden ubicarse en infraestructuras públicas o en los propios «drones patrulla», pueden detectar comportamientos sospechosos en tiempo real, alertando a las autoridades y permitiendo una respuesta más rápida ante un ilícito o un simple accidente fortuito. Además, pueden ayudar en la identificación y seguimiento de personas desaparecidas.

Por otra parte, la IA es una herramienta poderosa para el análisis de datos orientado a la prevención del crimen; La IA puede analizar grandes volúmenes de datos para identificar

patrones y tendencias delictivas, ayudando a las fuerzas de seguridad a anticipar y prevenir actividades criminales. La puesta en marcha de estos mecanismos exige una perfecta coordinación entre las fuerzas y cuerpos de seguridad, donde la policía local tiene sus propias competencias, pero la entidad pública puede colaborar en cuestiones importantes como la prevención del delito.

Aunque la seguridad no sea exclusivamente responsabilidad de las entidades públicas, el uso estratégico de la inteligencia artificial puede marcar una diferencia significativa. Al combinar herramientas avanzadas como la videovigilancia inteligente el análisis de datos predictivo, las administraciones
publicas pueden contribuir de manera sustancial a la construcción de entornos más seguros y a la mejora de la calidad.

"Los algoritmos de IA pueden mejorar la gestión de semáforos, predecir congestiones y proporcionar rutas más eficientes para el transporte público, lo que reduce la congestión y mejora la movilidad".

6. Optimización del tráfico y del transporte publico

En áreas urbanas, la IA se utiliza para optimizar el tráfico y el transporte público. Los algoritmos de IA pueden mejorar la gestión de semáforos, predecir congestiones y proporcionar rutas más eficientes para el transporte público, lo que reduce la congestión y mejora la movilidad.

Una de las aplicaciones más destacadas de la IA en este ámbito es la implementación de sistemas de gestión del tráfico en tiempo real; Utilizando algoritmos de aprendizaje automático y datos de sensores de tráfico, cámaras y dispositivos GPS, los Ayuntamientos pueden optimizar el flujo de vehículos y reducir los atascos. Por ejemplo, los semáforos inteligentes pueden adaptarse dinámicamente a las condiciones del tráfico, minimizando el tiempo de espera.

Otra área clave donde la IA está marcando la diferencia es en la predicción y planificación del transporte público. Mediante el uso de estos sistemas se pueden identificar tendencias como el aumento del número de pasajeros en determinadas líneas durante horas pico o eventos especiales. Con esta información, las administraciones locales pueden ajustar los horarios y frecuencias de los autobuses o metros para garantizar que haya suficiente capacidad para satisfacer la demanda. Además, los algoritmos sugieren pueden rutas alternativas o incluso rediseñar los trayectos para optimizar los tiempos de viaje y reducir costos de operación.

La integración de la IA en la gestión del tráfico y el transporte público tiene implicaciones que van más allá de la eficiencia operativa. Estas tecnologías también desempeñan un papel crucial en la planificación estratégica de las ciudades. Los datos recopilados por los sistemas inteligentes proporcionan información valiosa sobre los patrones de movilidad, lo que permite tomar decisiones informadas sobre inversiones en infraestructura, como la construcción de nuevas vías, carriles exclusivos para autobuses o estaciones de transporte público[1].

7. Detección y respuestas a desastres naturales

La IA puede ayudar en la detección temprana de desastres naturales, como terremotos, inundaciones e incendios forestales, y en la coordinación de la respuesta de emergencia, lo que puede salvar vidas y reducir el impacto.

Uno de los mayores desafíos en la prevención de desastres naturales es la capacidad de predecir cuándo y dónde ocurrirán. La IA desempeña un papel fundamental en la predicción de estos eventos al analizar datos históricos y en tiempo real. Por ejemplo, los algoritmos de aprendizaje automático pueden procesar datos meteorológicos, geológicos y sísmicos para identificar patrones que sugieran la probabilidad de un desastre inminente.

Los modelos de IA pueden detectar cambios sutiles en estas variables y emitir alertas tempranas a las autoridades y la población en riesgo. Esto permite la planificación anticipada de evacuaciones, la preparación de recursos y la reducción de daños humanos y materiales.

La IA no solo se utiliza para predecir desastres, sino que también monitorea de manera constante las áreas de alto riesgo. Los sistemas de monitoreo basados en IA pueden detectar cambios en las condiciones geológicas, climáticas y ambientales que podrían indicar la inminencia de un desastre. Por ejemplo, los sistemas de monitoreo de deslizamientos de tierra pueden identificar movimientos del suelo y alertar a las comunidades en riesgo.

"Uno de los mayores desafíos en la prevención de desastres naturales es la capacidad de predecir cuándo y dónde ocurrirán. La IA desempeña un papel fundamental en la predicción de estos eventos al analizar datos históricos y en tiempo real.".

[1] Víctor Almonacid, (19 de mayo, 2024) articulo*, "Smart City 2024: ejemplos de #IA aplicada a los servicios municipales"*.

"Drones equipados con algoritmos de IA pueden llevar a cabo una vigilancia constante de las áreas forestales, detectando señales de posibles fuentes de ignición, como relámpagos o fuegos provocados".

Este monitoreo continuo proporciona información valiosa que ayuda a las autoridades a tomar decisiones informadas y a las personas a estar preparadas en caso de emergencia.

Ejemplos prácticos del uso de la IA en la prevención de desastres naturales los encontramos en primer lugar, en la actividad sísmica. Particularmente los terremotos representan una catástrofe natural devastadora que ha sido objeto de una creciente atención en la comunidad científica. La Inteligencia Artificial se ha convertido en una herramienta esencial para mejorar nuestra comprensión y capacidad de predicción de estos eventos. Los modelos de aprendizaje automático se dedican a analizar datos sísmicos históricos, observar movimientos terrestres y detectar cambios sutiles en la corteza terrestre. Aunque no podemos predecir con precisión cuándo y dónde ocurrirán los terremotos, la detección puede otorgar a la población valiosos segundos para tomar medidas de seguridad y así minimizar el riesgo de pérdidas humanas.

En los últimos años, también hay que tener en cuenta que los incendios forestales han experimentado un alarmante aumento en términos de frecuencia e intensidad. La IA desempeña un papel crucial en la prevención de estos devastadores desastres. Drones equipados con algoritmos de IA pueden llevar a cabo una vigilancia constante de las áreas forestales, detectando señales de posibles fuentes de ignición, como relámpagos o fuegos provocados. Además, la IA tiene la capacidad de analizar datos meteorológicos para prever la propagación de los incendios, lo que proporciona a los servicios de extinción de incendios la información necesaria para desarrollar estrategias más efectivas en la lucha contra el fuego.

8. Planificación urbana y gestión de los residuos y saneamiento

La IA se puede utilizar en la planificación urbana para optimizar el uso de recursos, prever necesidades de infraestructura y gestionar eficientemente los residuos y la energía en las ciudades.

"Otro ámbito en el que la IA está marcando la diferencia es la gestión y mantenimiento de las redes de saneamiento. Las infraestructuras de agua y alcantarillado son esenciales para garantizar la salud pública y la calidad de vida, pero a menudo enfrentan problemas como bloqueos, fugas o desgaste estructural. La IA, combinada con sensores inteligentes, ofrece una solución innovadora a este tipo de problemas en las infraestructuras".

Uno de los mayores avances que la IA aporta a la gestión de residuos es la posibilidad de optimizar las rutas de recolección de basura. Utilizando datos históricos sobre los patrones de llenado de los contenedores y datos en tiempo real recopilados por sensores instalados en estos mismos, los algoritmos de IA pueden diseñar itinerarios más eficientes para los camiones recolectores. Este enfoque tiene múltiples beneficios. Por un lado, permite reducir significativamente el consumo de combustible al acortar las distancias recorridas y evitar rutas innecesarias. Por otro lado, disminuye las emisiones de carbono asociadas al transporte, lo que contribuye directamente a mitiga.

Además, los contenedores inteligentes desempeñan un papel fundamental en este proceso. Equipados con sensores avanzados, estos dispositivos son capaces de medir el nivel de llenado de cada contenedor, proporcionando datos clave para priorizar la recolección donde más se necesita. Por ejemplo, en lugar de seguir una ruta fija y recoger todos los contenedores, los camiones pueden dirigirse primero a aquellos que están completamente llenos, evitando desplazamientos innecesarios.

Otro ámbito en el que la IA está marcando la diferencia es la gestión y mantenimiento de las redes de saneamiento. Las infraestructuras de agua y alcantarillado son esenciales para garantizar la salud pública y la calidad de vida, pero a menudo enfrentan problemas como bloqueos, fugas o desgaste estructural. La IA, combinada con sensores inteligentes, ofrece una solución innovadora a este tipo de problemas en las infraestructuras. Esto facilita un mantenimiento predictivo, minimizando interrupciones y costos de reparación.

9. Planificación urbanística y medio ambiente

La IA tiene el potencial de generar impactos positivos significativos en múltiples áreas relacionadas con la planificación urbanística y el medio ambiente. Aunque existen iniciativas avanzadas como los «gemelos digitales», que ofrecen una representación virtual detallada de las ciudades y permiten realizar análisis complejos, en esta ocasión nos centraremos en otras aplicaciones igualmente valiosas que están transformando la gestión urbana.

"Otro campo en el que la IA demuestra ser invaluable es en el monitoreo ambiental; Sensores y análisis de datos en tiempo real permiten a la administración pública monitorear la calidad del aire, el ruido y otros factores ambientales, facilitando una gestión proactiva y sostenible del entorno urbano."

Una de las contribuciones más destacadas de la IA en el ámbito de la planificación urbana es la capacidad para realizar simulaciones y modelados predictivos.

Gracias a estas simulaciones, los planificadores urbanos pueden tomar decisiones más informadas y basadas en evidencia. En lugar de depender únicamente de estimaciones o estudios manuales, los algoritmos ofrecen una visión más completa y precisa de los posibles resultados, lo que reduce el margen de error y mejora la eficacia de las políticas urbanas. Esto es especialmente relevante en decisiones críticas como la construcción de infraestructuras, la distribución del suelo para usos residenciales o comerciales, y la planificación de segmentos urbanos.
Otro campo en el que la IA demuestra ser invaluable es en el monitoreo ambiental; Sensores y análisis de datos en tiempo real permiten a la administración pública monitorear la calidad del aire, el ruido y otros factores ambientales, facilitando una gestión proactiva y sostenible del entorno urbano.

Por ejemplo, si los sensores detectan un aumento significativo en los niveles de partículas contaminantes en el aire, los sistemas de IA pueden alertar a las autoridades locales para que implementen medidas correctivas, como restricciones al tráfico o campañas de concienciación. Asimismo, los análisis en tiempo real pueden ayudar a mitigar el impacto de actividades industriales o eventos masivos que pueden generar contaminación, promoviendo una gestión

Estas herramientas refuerzan la capacidad de las ciudades para adaptarse a desafíos globales como el cambio climático, la urbanización acelerada y la gestión eficiente de recursos. La IA no solo ayuda a identificar problemas, sino que también ofrece soluciones prácticas para abordarlos, contribuyendo a la construcción de ciudades más inteligentes, habitables y sostenibles.

1.2. Ejemplos reales

A continuación, detallamos algunos de estos ejemplos:

- El Ayuntamiento de Alicante, caso de éxito en la aplicación de la inteligencia artificial a través de la compra pública de innovación

". El proyecto busca reducir la brecha digital y mejorar la accesibilidad a la administración, con la posibilidad de incorporar modelos predictivos para la toma de decisiones. Además, actúa como un referente en la compra pública de innovación, promoviendo la internacionalización de las empresas que participaron en su desarrollo".

El Ayuntamiento de Alicante ha lanzado un proyecto innovador basado en la compra pública de innovación (CPI), denominado ALI. Esta herramienta, impulsada por inteligencia artificial (IA), tiene como objetivo facilitar a los ciudadanos el acceso y la realización de trámites a través de la sede electrónica del municipio. Utiliza un asistente virtual que responde a dudas y anticipa necesidades, mejorando la interacción con la administración.

Desarrollada por las empresas Lynx View y Efor Global Technology, ALI es pionera en España y se encuentra disponible en el portal ali.alicante.es. El sistema ha sido entrenado con datos de 100.000 llamadas al servicio municipal 010 y ha sido financiado con fondos europeos, con apoyo de la Agencia Valenciana de Innovación. El proyecto busca reducir la brecha digital y mejorar la accesibilidad a la administración, con la posibilidad de incorporar modelos predictivos para la toma de decisiones. Además, actúa como un referente en la compra pública de innovación, promoviendo la internacionalización de las empresas que participaron en su desarrollo.

Consulta la noticia en este enlace.

- AviBot, el asistente virtual por inteligencia artificial del Ayuntamiento de Avilés ya está disponible para consultas y trámites

El Ayuntamiento de Avilés ha lanzado su asistente virtual 'AviBot', cuyo objetivo es mejorar el acceso a servicios públicos de manera rápida y eficiente. Funciona las 24 horas del día y utiliza Inteligencia Artificial para interpretar el lenguaje humano, respondiendo preguntas y guiando a los usuarios en trámites como citas previas, consultas de incidencias, o disponibilidad de bicicletas.

AviBot está disponible en canales como la web municipal, WhatsApp, Telegram y teléfono, y responde tanto a preguntas predefinidas como a consultas libres sobre diversos servicios del Ayuntamiento. Fue desarrollado por la empresa One Million Bot S.L. con una inversión de 88.273,13 euros, cofinanciada por el Fondo Europeo de Desarrollo Regional. Además, está disponible en español y asturiano.

"Ell chatbot aprende de cada interacción gracias a su inteligencia artificial y el análisis de datos, mejorando continuamente la experiencia del usuario. Este proyecto está cofinanciado por fondos europeos y forma parte de la Estrategia de Desarrollo Urbano Sostenible de Torrent".

Consulta la noticia en este enlace.

- 'Llum', el nuevo asistente virtual para la ciudadanía de Torrent

El Ayuntamiento de Torrent ha lanzado 'Llum', un chatbot inteligente disponible 24/7 en su página web para asistir a los usuarios en sus trámites y consultas. Desarrollado por '1millionbot', ofrece respuestas rápidas a dudas comunes sobre servicios municipales como empadronamiento, incidencias o domiciliación de recibos. Esta herramienta busca mejorar la interacción con la administración, optimizando la experiencia de los ciudadanos sin reemplazar otros medios de atención, como la presencial.

Durante su fase de pruebas en noviembre y diciembre, 'Llum' atendió más de 1600 consultas con una tasa de acierto superior al 90%. Además, el chatbot aprende de cada interacción gracias a su inteligencia artificial y el análisis de datos, mejorando continuamente la experiencia del usuario. Este proyecto está cofinanciado por fondos europeos y forma parte de la Estrategia de Desarrollo Urbano Sostenible de Torrent.

Consulta la noticia en este enlace.

- El Ayuntamiento de Valladolid presenta a 'ANA', la asistente virtual inteligente de su nueva web municipal.

Se trata de un chatbot pionero en su ámbito a nivel nacional, basado 100% en inteligencia artificial generativa, que asiste a la ciudadanía ante preguntas de diversa tipología vinculadas a las competencias municipales. Esta herramienta fue desarrollada por los técnicos del Ayuntamiento en colaboración con Luce IT una empresa vallisoletana.

Como dato curioso, cuenta la noticia que la elección de 'ANA' como nombre para el asistente, es en honor a la empleada municipal que mantiene la base de datos de atención ciudadana desde hace décadas.

Consulta la noticia en este enlace.

""El Ayuntamiento de Madrid ha lanzado un proyecto piloto llamado 'Paloma', que utiliza Inteligencia Artificial (IA) para identificar y apoyar a personas mayores en situación de soledad no deseada. Entre el 28 de noviembre y el 8 de diciembre de 2023, se contactó a 5.163 mayores de 75 años que viven solos, a través de un asistente virtual inteligente".

- "Javi" el asistente virtual del Ayuntamiento de San Javier.

El Ayuntamiento de San Javier (Murcia) ha creado un Chatbot de IA, que ejerce como asistente virtual a través de la web municipal. El asistente virtual, apodado como "Javi", atiende hasta en 80 idiomas y resuelve en segundos cualquier pregunta sobre temas burocráticos del propio Ayuntamiento como de información general relacionada con Educación, Sanidad, temas sociales o cualquier otro relacionado con el municipio.

Con esta iniciativa han querido conseguir dar accesibilidad del ciudadano a la información municipal combatiendo la brecha digital por su fácil usabilidad y además incorpora hasta 80 idiomas de respuesta, ya que en el municipio de San Javier hay vecinos empadronados de 200 nacionalidades. El ayuntamiento explica que el chatbot se nutre de más de 500 URL y 350 documentos en su base de datos para poder ofrecer respuestas concisas a cualquier pregunta.

Consulta la noticia en este enlace.

- Madrid inicia la atención social a más de 600 mayores en soledad no deseada detectados mediante Inteligencia Artificial

El Ayuntamiento de Madrid ha lanzado un proyecto piloto llamado 'Paloma', que utiliza Inteligencia Artificial (IA) para identificar y apoyar a personas mayores en situación de soledad no deseada. Entre el 28 de noviembre y el 8 de diciembre de 2023, se contactó a 5.163 mayores de 75 años que viven solos, a través de un asistente virtual inteligente. El 31% de las mujeres y el 34% de los hombres manifestaron sentirse solos, aunque muchos contaban con una red de apoyo. El proyecto no solo identificó a los mayores que se sentían solos, sino que también inició una segunda fase de seguimiento social personalizado, atendiendo a 602 personas mediante un programa de acompañamiento social, que incluyó visitas domiciliarias a 143 de ellas. Aquellos con mayor riesgo de vulnerabilidad fueron atendidos por los Servicios Sociales. Esta intervención, que involucró más de 113 horas de diálogo, ha permitido brindar un apoyo integral

“El sistema automatizado permitirá a los profesionales conocer en tiempo real el estado de las licencias de urbanismo y asegurarse de que cumplen con los requisitos de forma eficiente, reduciendo la carga de trabajo de los empleados municipales y acelerando los trámites”.

y personalizado a los mayores, mejorando la detección y respuesta a la soledad no deseada gracias al uso de la IA.

Consulta la noticia en este enlace.

- El Ayuntamiento de Madrid utilizará inteligencia artificial para "generar licencias de urbanismo"

El Ayuntamiento de Madrid está implementando Inteligencia Artificial (IA) para agilizar la gestión de licencias urbanísticas, facilitando tanto el trabajo de los técnicos como el de los arquitectos. El sistema automatizado permitirá a los profesionales conocer en tiempo real el estado de las licencias de urbanismo y asegurarse de que cumplen con los requisitos de forma eficiente, reduciendo la carga de trabajo de los empleados municipales y acelerando los trámites. Esta iniciativa se enmarca dentro de un contexto de alta demanda de vivienda en la ciudad, tanto pública como privada.

Además de este proyecto, el Ayuntamiento está colaborando en otras iniciativas tecnológicas, como un bastón para personas ciegas que les permite conocer lo que ocurre a su alrededor mediante pitidos. También han creado el grupo de trabajo 'MAIA', compuesto por diversas áreas del Consistorio, para aplicar soluciones basadas en IA y mejorar la eficiencia de los servicios públicos y la comunicación con los ciudadanos. Esto incluye herramientas que facilitan la interacción con el Ayuntamiento y optimizan el trabajo burocrático de los empleados públicos, mejorando la gestión y los servicios en la ciudad.

Consulta la noticia en este enlace.

- El Ayuntamiento de Granada firma un acuerdo de colaboración con Orange para impulsar el primer Centro Demostrador de IA Urbana en España

La alcaldesa de Granada, y el director de Orange en Andalucía, firmaron un convenio para colaborar en el “Centro Demostrador de Inteligencia Artificial Urbano iQuantum”. Este centro, el primero de su tipo en España, abrirá en 2025 y se centrará en el desarrollo de soluciones tecnológicas para mejorar la eficiencia de las administraciones públicas.

"Este proyecto, clave para la Comisión Europea, tiene como objetivo aplicar la Inteligencia Artificial en la gestión urbana para transformar los servicios municipales. València coordina el supernodo sur de Europa y busca posicionarse como líder en innovación digital. Además, tras los efectos de la DANA, el Ayuntamiento ha encargado a los socios del proyecto desarrollar soluciones para la recuperación. Citcom.AI mejorará áreas como sostenibilidad, gestión de ruido y residuos, y busca ser un referente europeo en ciudades inteligentes y sostenibles".

Además, ofrecerá formación en IA y sesiones para empresas. El centro contará con la participación de diversas entidades, incluyendo empresas, universidades y administraciones públicas.

Consulta la noticia en este enlace.

- València contratará una oficina técnica para liderar la inteligencia artificial urbana con el proyecto Citcom.AI

El Ayuntamiento de València ha contratado una oficina de asistencia técnica para el proyecto Citcom.AI, con una inversión de 600.000 euros. Este proyecto, clave para la Comisión Europea, tiene como objetivo aplicar la Inteligencia Artificial en la gestión urbana para transformar los servicios municipales. València coordina el supernodo sur de Europa y busca posicionarse como líder en innovación digital. Además, tras los efectos de la DANA, el Ayuntamiento ha encargado a los socios del proyecto desarrollar soluciones para la recuperación. Citcom.AI mejorará áreas como sostenibilidad, gestión de ruido y residuos, y busca ser un referente europeo en ciudades inteligentes y sostenibles.

Consulta la noticia en este enlace.

2. PRINCIPALES CUESTIONES LEGALES EN APLICACIÓN DEL REGLAMENTO EUROPEO DE INTELIGENCIA ARTIFICIAL (RIA)

2.1. Plazos para la adecuacion al RIA

En primer lugar, interesa saber qué plazos prevé el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante, Reglamento de Inteligencia Artificial o RIA), a fin de atender al cumplimiento de cuanto en él se recoge.

Como se muestra, a continuación, existen una diversidad de plazos, de los cuales se señalarán los más significativos para autoridad pública, órgano u organismo, esto es, para la Administración pública, en general.

"el Considerando 179 indica lo siguiente: El presente Reglamento debe aplicarse a partir del 2 de agosto de 2026. No obstante, teniendo en cuenta el riesgo inaceptable asociado a determinadas formas de uso de la IA, las prohibiciones, así como las disposiciones generales del presente Reglamento, deben aplicarse ya desde el 2 de febrero de 2025".

Por un lado, el artículo 113 del RIA establece un plazo de entrada en vigor de veinte días desde su publicación en el Diario Oficial de la Unión Europea, plazo que finalizó el pasado 1 de agosto de 2024. No obstante, el mismo precepto concede un plazo de dos años hasta su plena aplicación, por lo que el RIA será aplicable a partir del 2 de agosto de 2026, aunque con una serie de salvedades:

- Los capítulos I (Disposiciones generales) y II (prácticas de IA prohibidas) serán aplicables a partir del 2 de febrero de 2025 [art. 113.a) RIA].

A este respecto, el Considerando 179 indica lo siguiente: *"El presente Reglamento debe aplicarse a partir del 2 de agosto de 2026. No obstante, teniendo en cuenta el riesgo inaceptable asociado a determinadas formas de uso de la IA, las prohibiciones, así como las disposiciones generales del presente Reglamento, deben aplicarse ya desde el 2 de febrero de 2025. Aunque dichas prohibiciones no surtan pleno efecto hasta después del establecimiento de la gobernanza y la aplicación del presente Reglamento, es importante anticipar la aplicación de las prohibiciones para tener en cuenta los riesgos inaceptables y adaptar otros procedimientos, por ejemplo, en el ámbito del Derecho civil. Además, la infraestructura relacionada con la gobernanza y el sistema de evaluación de la conformidad deben estar operativos antes de esa fecha, por lo que las disposiciones relativas a los organismos notificados y la estructura de gobernanza deben ser aplicables a partir del 2 de agosto de 2026. Dada la rápida evolución tecnológica y el elevado ritmo de adopción de modelos de IA de uso general, las obligaciones de los proveedores de modelos de IA de uso general deben aplicarse desde el 2 de agosto de 2025. Los códigos de buenas prácticas deben estar finalizados a más tardar el 2 de mayo de 2025 al objeto de permitir a los proveedores demostrar el cumplimiento de sus obligaciones dentro del plazo previsto. La Oficina de IA debe velar por que las normas y los procedimientos de clasificación estén actualizados con arreglo a los avances tecnológicos. Asimismo, los Estados miembros deben establecer y poner en conocimiento de la Comisión las normas referentes a las sanciones, incluidas las multas administrativas, y asegurarse*

de que para la fecha de aplicación del presente Reglamento se apliquen de manera adecuada y efectiva. Por lo tanto, las disposiciones relativas a las sanciones deben aplicarse a partir del 2 de agosto de 2025".

- El capítulo III, sección 4 (Autoridades notificantes y organismos notificados), el capítulo V (Modelos de IA de uso general), el capítulo VII (Gobernanza) y el capítulo XII (Sanciones) y el artículo 78 (Confidencialidad) serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101 (Multas a proveedores de modelos de IA de uso general) [art. 113.a) RIA].

- El artículo 6, apartado 1 (Condiciones IA de alto riesgo), y las obligaciones correspondientes del Reglamento serán aplicables a partir del 2 de agosto de 2027.

Asimismo, hallamos en el RIA otros preceptos que establecen diferentes plazos de aplicación:

- Los sistemas de IA que sean componentes de los sistemas informáticos de gran magnitud enumerados en el anexo X y que se hayan introducido en el mercado o se hayan puesto en servicio antes del 2 de agosto de 2027 deberán estar en conformidad con el Reglamento a más tardar el 31 de diciembre de 2030 [art. 111.1 RIA].

- Una de las excepciones que han de tener muy presente las AA.PP. es la de los **proveedores y los responsables del despliegue de los sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas**, que deberán adoptar las medidas necesarias para cumplir los requisitos y obligaciones del Reglamento a más tardar el **2 de agosto de 2030** [Considerando 177 *in fine*; art. 111.2 RIA]. En el próximo apartado examinaremos cuáles son considerados "sistemas de IA de alto riesgo".
- Los proveedores de modelos de IA de uso general que se hayan introducido en el mercado antes del 2 de agosto de 2025 deben adoptar las medidas necesarias para cumplir las obligaciones establecidas en el Reglamento a más tardar el 2 de agosto de 2027 [art. 111.3 RIA].

"Una de las excepciones que han de tener muy presente las AA.PP. es la de los proveedores y los responsables del despliegue de los sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas, que deberán adoptar las medidas necesarias para cumplir los requisitos y obligaciones del Reglamento a más tardar el 2 de agosto de 2030".

Apunta la AVPD que la habilitación para grabar los plenos tampoco alcanzaría los casos en que la corporación haya hecho uso de la facultad de declarar secreto el debate y votación por afectarse al honor e intimidad de los ciudadanos.

Por último, recuerda que el cumplimiento del principio de transparencia proclamado en el art 5.1.a) del RGPD exige que los asistentes al pleno sean informados de que la sesión será grabada y difundida, en los términos exigidos por la normativa en materia de protección de datos.

2.2. Roles de la AA.PP. (Proveedor; responsable del despliegue o implementador; distribuidor; importador) entorno a la IA

En el artículo 3 del RIA se encuentran las definiciones de los roles que pueden asumir las distintas partes (personas físicas o jurídicas) a las que les resulta de aplicación el Reglamento, y que pueden implicar a las AA.PP. y sus contratistas. En el presente apartado se describirán los roles más significativos:

- Proveedor:

"Una persona física o jurídica o autoridad, órgano u organismo de otra índole públicos que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca comercial, previo pago o gratuitamente". [Art. 3.3 RIA]

Un ejemplo de proveedor bajo los términos del Reglamento es OpenAI, la empresa detrás de sistemas de IA muy conocidos como ChatGPT, que se han puesto a servicio de los usuarios finales en modalidad tanto gratuita como de pago.

"Un ejemplo de proveedor bajo los términos del Reglamento es OpenAI, la empresa detrás de sistemas de IA muy conocidos como ChatGPT, que se han puesto a servicio de los usuarios finales en modalidad tanto gratuita como de pago".

- Responsable del despliegue o implementador:

"Toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se

enmarque en una actividad personal de carácter no profesional". [Art. 3.4 RIA]

Cabe precisar que el responsable del despliegue no es la persona física que acaba usando el sistema de IA, sino la persona o entidad que implementa dicho sistema para su uso. A título ilustrativo, si una entidad despliega un sistema de IA para que pueda ser utilizado por sus empleados, dicha entidad será la responsable del despliegue de dicho sistema, mientras que los empleados serán los usuarios finales del mismo. **Así, el de responsable del despliegue será el rol que más frecuentemente asuman las AA.PP., especialmente en el ámbito de la Administración Local.**

"Toda persona física o jurídica ubicada o establecida en la Unión que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor".

- Representante autorizado:

"Toda persona física o jurídica ubicada o establecida en la Unión que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor". [Art. 3.5 RIA]

El representante autorizado es, por tanto, una persona ubicada en el territorio de la Unión Europea que deberá ser designada por aquellos proveedores que se encuentren fuera de dicho territorio para que cumpla las obligaciones y lleve a cabo las acciones exigidas por el RIA en su nombre.

El rol de representante autorizado podría equipararse a la figura del "representante" en el marco del Reglamento General de Protección de Datos (Art. 4.17, RGPD).

- Importador:

"Una persona física o jurídica ubicada o establecida en la Unión que introduzca en el mercado un sistema de IA que lleve el nombre o la marca comercial de una persona física o jurídica establecida en un tercer país". [Art. 3.6 RIA]

"Una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión".

Tal y como se extrae de la propia definición, el importador es aquella persona establecida dentro del territorio de la Unión Europea que comercializa o pone en servicio un sistema de IA bajo el nombre o marca comercial de otra persona establecida fuera del territorio europeo.

- Distribuidor:

"Una persona física o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice un sistema de IA en el mercado de la Unión". [Art. 3.7 RIA]

El distribuidor, a diferencia del importador, será cualquier otro sujeto en la cadena de suministro de un sistema de IA que comercialice el sistema, siempre que no tenga el rol de importador o que no influya sobre las propiedades del sistema. Cabe destacar, en cualquier caso, que el RIA impone distintas obligaciones a los distribuidores y a los importadores, al estar involucrados en diferentes etapas de la cadena de suministro.

- Operador:

"Un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor". [Art. 3.8 RIA]

Como se aprecia de la propia definición del RIA, "Operador" es un término amplio que comprende prácticamente la totalidad de los roles previamente definidos.

2.3. Categorizacion de los sitemas de IA

Antes de entrar a examinar las concretas obligaciones que les atribuye el RIA, hemos de precisar que este Reglamento europeo categoriza los sistemas de IA según el riesgo que estos conllevan para los derechos fundamentales de las personas, existiendo sistemas de riesgo inaceptable, de alto riesgo, de riesgo limitado y de riesgo mínimo.

"también se consideran de alto riesgo los sistemas de IA contemplados en el Anexo III del RIA (biometría; infraestructuras críticas; educación y formación profesional; empleo, gestión de los trabajadores y acceso al autoempleo; acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de los mismos; garantía del cumplimiento del Derecho; migración, asilo y gestión del control fronterizo; Administración de justicia y procesos democráticos)".

En el presente, nos centraremos en los considerados "sistemas de IA de alto riesgo", pues es en el uso de estos donde el RIA establece unos requisitos y obligaciones más estrictos. Las **reglas de clasificación de los sistemas de IA como "sistemas de alto riesgo"** son las establecidas en el artículo 6 del RIA:

Con independencia de si se ha introducido en el mercado o se ha puesto en servicio, un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación:

a) que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión enumerados en el anexo I, o que el propio sistema de IA sea uno de dichos productos, y

b) que el producto del que el sistema de IA sea componente de seguridad con arreglo a la letra a), o el propio sistema de IA como producto, deba someterse a una evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio con arreglo a los actos legislativos de armonización de la Unión enumerados en el anexo I.

Además de los sistemas de IA de alto riesgo anteriores, también se consideran de alto riesgo los sistemas de IA contemplados en el Anexo III del RIA (biometría; infraestructuras críticas; educación y formación profesional; empleo, gestión de los trabajadores y acceso al autoempleo; acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de los mismos; garantía del cumplimiento del Derecho; migración, asilo y gestión del control fronterizo; Administración de justicia y procesos democráticos). Nos detendremos, en este punto, en el detalle de los ámbitos de "acceso a servicios públicos esenciales" y "migración, asilo y gestión del control fronterizo". Así, serán sistemas de IA de alto riesgo con arreglo al artículo 6.2 RIA, los que formen parte de:

"Sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar la admisibilidad de las personas físicas para beneficiarse de servicios y prestaciones esenciales de asistencia pública, incluidos los servicios de asistencia sanitaria, así como para conceder, reducir o retirar dichos servicios y prestaciones o reclamar su devolución."

○ Acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de estos servicios y prestaciones [Anexo III. 5]:

a) Sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para evaluar la admisibilidad de las personas físicas para beneficiarse de servicios y prestaciones esenciales de asistencia pública, incluidos los servicios de asistencia sanitaria, así como para conceder, reducir o retirar dichos servicios y prestaciones o reclamar su devolución.

b) Sistemas de IA destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su calificación crediticia, salvo los sistemas de IA utilizados al objeto de detectar fraudes financieros.

c) Sistemas de IA destinados a ser utilizados para la evaluación de riesgos y la fijación de precios en relación con las personas físicas en el caso de los seguros de vida y de salud.

d) Sistemas de IA destinados a ser utilizados para la evaluación y la clasificación de las llamadas de emergencia realizadas por personas físicas o para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, por ejemplo, policía, bomberos y servicios de asistencia médica, y en sistemas de triaje de pacientes en el contexto de la asistencia sanitaria de urgencia.

En particular, las personas físicas que solicitan a las autoridades públicas o reciben de estas prestaciones y servicios esenciales de asistencia pública, a saber, servicios de asistencia sanitaria, prestaciones de seguridad social, servicios sociales que garantizan una protección en casos como la maternidad, la enfermedad, los accidentes laborales, la dependencia o la vejez y la pérdida de empleo, asistencia social y ayudas a la vivienda, suelen depender de dichas prestaciones y servicios y, por lo general, se encuentran en una posición de vulnerabilidad respecto de las autoridades responsables. La utilización de sistemas de IA

"también se consideran de alto riesgo los sistemas de IA contemplados en el Anexo III del RIA (biometría; infraestructuras críticas; educación y formación profesional; empleo, gestión de los trabajadores y acceso al autoempleo; acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de los mismos; garantía del cumplimiento del Derecho; migración, asilo y gestión del control fronterizo; Administración de justicia y procesos democráticos)".

para decidir si las autoridades deben conceder, denegar, reducir o revocar dichas prestaciones y servicios o reclamar su devolución, lo que incluye decidir, por ejemplo, si los beneficiarios tienen legítimamente derecho a dichas prestaciones y servicios, podría tener un efecto considerable en los medios de subsistencia de las personas y vulnerar sus derechos fundamentales, como el derecho a la protección social, a la no discriminación, a la dignidad humana o a la tutela judicial efectiva y, por lo tanto, deben clasificarse como de alto riesgo. No obstante, el presente RIA no debe obstaculizar el desarrollo y el uso de enfoques innovadores en la Administración, que podrían beneficiarse de una mayor utilización de sistemas de IA conformes y seguros, siempre y cuando dichos sistemas no supongan un alto riesgo para las personas jurídicas y físicas [Considerando 58 RIA].

- <u>Migración, asilo y gestión del control fronterizo, en la medida en que su uso esté permitido por el Derecho de la Unión o nacional aplicable [Anexo III. 7]:</u>

a) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión, como polígrafos o herramientas similares.

b) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión para evaluar un riesgo, por ejemplo, un riesgo para la seguridad, la salud o de migración irregular, que plantee una persona física que tenga la intención de entrar en el territorio de un Estado miembro o haya entrado en él.

c) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión para ayudar a las autoridades públicas competentes a examinar las solicitudes de asilo, visado o permiso de residencia y las reclamaciones conexas con el fin de determinar si las personas físicas solicitantes reúnen los requisitos necesarios para que se conceda su solicitud, con

"También se consideran de alto riesgo los sistemas de IA contemplados en el Anexo III del RIA (biometría; infraestructuras críticas; educación y formación profesional; empleo, gestión de los trabajadores y acceso al autoempleo; acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de los mismos; garantía del cumplimiento del Derecho; migración, asilo y gestión del control fronterizo; Administración de justicia y procesos democráticos)".

inclusión de la evaluación conexa de la fiabilidad de las pruebas.

d) Sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos y organismos de la Unión, en el contexto de la migración, el asilo o la gestión del control fronterizo, con el fin de detectar, reconocer o identificar a personas físicas, con excepción de la verificación de documentos de viaje.

Los sistemas de IA empleados en la migración, el asilo y la gestión del control fronterizo afectan a personas que con frecuencia se encuentran en una situación especialmente vulnerable y que dependen del resultado de las actuaciones de las autoridades públicas competentes. Por este motivo, es sumamente importante que los sistemas de IA que se utilicen en estos contextos sean precisos, no discriminatorios y transparentes, a fin de garantizar que se respeten los derechos fundamentales de las personas afectadas y, en particular, su derecho a la libre circulación, a la no discriminación, a la intimidad personal y la protección de los datos personales, a la protección internacional y a una buena administración. Por lo tanto, procede clasificar como de alto riesgo, en la medida en que su utilización esté permitida en virtud del Derecho de la Unión y nacional, aquellos sistemas de IA destinados a ser utilizados por las autoridades públicas competentes, o en su nombre, o por las instituciones, órganos u organismos de la Unión que realizan tareas en el ámbito de la migración, el asilo y la gestión del control fronterizo como polígrafos y herramientas similares, para evaluar determinados riesgos que presenten las personas físicas que entren en el territorio de un Estado miembro o que soliciten un visado o asilo, para ayudar a las autoridades públicas competentes a examinar, con inclusión de la evaluación conexa de la fiabilidad de las pruebas, las solicitudes de asilo, visado y permiso de residencia, así como las reclamaciones conexas en relación con el objetivo de determinar si las personas físicas solicitantes reúnen los requisitos necesarios para que se conceda su solicitud, a efectos de detectar, reconocer o identificar a las personas físicas en el contexto de la migración, el asilo y la gestión del

"también se consideran de alto riesgo los sistemas de IA contemplados en el Anexo III del RIA (biometría; infraestructuras críticas; educación y formación profesional; empleo, gestión de los trabajadores y acceso al autoempleo; acceso a servicios privados esenciales y a servicios y prestaciones públicos esenciales y disfrute de los mismos; garantía del cumplimiento del Derecho; migración, asilo y gestión del control fronterizo; Administración de justicia y procesos democráticos)".

control fronterizo, con excepción de la verificación de los documentos de viaje [Considerando 60 RIA].

No obstante, lo anterior, un sistema de IA no se considerará de alto riesgo cuando no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales de las personas físicas, también al no influir sustancialmente en el resultado de la toma de decisiones. Esto se aplicará cuando se cumpla cualquiera de las condiciones siguientes [art. 6.3 RIA]:

a) que el sistema de IA esté destinado a realizar una tarea de procedimiento limitada;

b) que el sistema de IA esté destinado a mejorar el resultado de una actividad humana previamente realizada;

c) que el sistema de IA esté destinado a detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la valoración humana previamente realizada sin una revisión humana adecuada, ni a influir en ella, o

d) que el sistema de IA esté destinado a realizar una tarea preparatoria para una evaluación que sea pertinente a efectos de los casos de uso enumerados en el anexo III.

Ahora bien, los sistemas de IA a que se refiere el Anexo III siempre se considerarán de alto riesgo cuando el sistema de IA efectúe la elaboración de perfiles de personas físicas.

2.4. Obligaciones y responsabilidades entes del sector público, según el rol en la IA

Las obligaciones y responsabilidades de los entes del sector público variarán en función de los riesgos implícitos en el sistema de IA de que se trate, así como del rol que asuman en cada caso. Tal y como apuntan CERRILLO I MARTINEZ, Agustí y VELASCO RICO, Clara I. en *"El Reglamento de la IA de la UE y competencias autonómicas",* las AA.PP. tienen reconocidas distintas funciones y responsabilidades en el RIA

"Una vez claras las reglas de clasificación de los sistemas de IA como "sistemas de alto riesgo", a continuación, procedemos a enumerar las distintas funciones y responsabilidades que las AA.PP. tienen reconocidas en el RIA y que, en términos generales, son las mismas que deberá cumplir cualquier persona o entidad que provea o sea responsable del despliegue de un sistema de IA".

que, en términos generales, son las mismas que deberá cumplir cualquier persona o entidad que provea o sea responsable del despliegue de un sistema de IA.

Una vez claras las reglas de clasificación de los sistemas de IA como "sistemas de alto riesgo", a continuación, procedemos a enumerar las distintas funciones y responsabilidades que las AA.PP. tienen reconocidas en el RIA y que, en términos generales, son las mismas que deberá cumplir cualquier persona o entidad que provea o sea responsable del despliegue de un sistema de IA.

- Las obligaciones de las AA.PP. como responsables del despliegue:

Las AA.PP. pueden ser responsables del despliegue, es decir, utilizar sistemas de IA bajo su propia autoridad [art. 3.4 RIA]. Las obligaciones que el RIA atribuye a los responsables del despliegue de sistemas de IA de alto riesgo son las siguientes:

- Adoptar medidas técnicas y organizativas adecuadas para garantizar que utilizan dichos sistemas con arreglo a las instrucciones de uso que los acompañen [art. 26.1 RIA].
- Encomendar la supervisión humana a personas físicas que tengan la competencia, la formación y la autoridad necesarias [art. 26.2 RIA].
- Asegurarse de que los datos de entrada sean pertinentes y suficientemente representativos en vista de la finalidad prevista del sistema de IA de alto riesgo, en la medida en que ejerza el control sobre dichos datos [art. 26.4 RIA].
- Vigilar el funcionamiento del sistema de IA de alto riesgo basándose en las instrucciones de uso y, cuando proceda, informar a los proveedores [art. 26.5 RIA]
- Conservar los archivos de registro que los sistemas de IA de alto riesgo generen automáticamente en la medida en que dichos archivos estén bajo su control, durante un período de tiempo adecuado para la finalidad prevista del sistema de IA de alto riesgo, de al menos seis meses, salvo que se disponga otra cosa en el Derecho de la Unión

"Concretamente, el art. 49.3 RIA 3 señala que antes de poner en servicio o utilizar un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 2, los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades públicas, instituciones, órganos u organismos de la Unión, o personas que actúen en su nombre, se registrarán, seleccionarán el sistema y registrarán su utilización en la base de datos correspondiente de la UE)".

o nacional aplicable, en particular en el Derecho de la Unión en materia de protección de datos personales [art. 26.6 RIA].

- Antes de poner en servicio o utilizar un sistema de IA de alto riesgo en el lugar de trabajo, los responsables del despliegue que sean empleadores deben informar a los representantes de los trabajadores y a los trabajadores afectados de que estarán expuestos a la utilización del sistema de IA de alto riesgo [art. 26.7 RIA].

- Los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades públicas o instituciones, órganos y organismos de la Unión deben cumplir con las obligaciones de registro a que se refiere el artículo 49 [art. 26.8 RIA]. Concretamente, el art. 49.3 RIA 3 señala que antes de poner en servicio o utilizar un sistema de IA de alto riesgo enumerado en el anexo III, con excepción de los sistemas de IA de alto riesgo mencionados en el anexo III, punto 2, los responsables del despliegue de sistemas de IA de alto riesgo que sean autoridades públicas, instituciones, órganos u organismos de la Unión, o personas que actúen en su nombre, se registrarán, seleccionarán el sistema y registrarán su utilización en la base de datos correspondiente de la UE.

- Cuando proceda, los responsables del despliegue de sistemas de IA de alto riesgo deben utilizar la información facilitada conforme al artículo 13 del RIA (transparencia y comunicación de información) para cumplir la obligación de llevar a cabo una evaluación de impacto relativa a la protección de datos que les imponen el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680 [art. 26.9 RIA].

- Los responsables del despliegue de los sistemas de IA de alto riesgo a que se refiere el anexo III que tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas deben informar a las personas físicas de que están expuestas a la utilización de los sistemas de IA de alto riesgo [art. 26.11 RIA].

"Toda persona que se vea afectada por una decisión que el responsable del despliegue adopte basándose en los resultados de salida de un sistema de IA de alto riesgo que figure en el anexo III, con excepción de los sistemas enumerados en su punto 2, y que produzca efectos jurídicos o le afecte considerablemente del mismo modo, de manera que considere que tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales, tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada [art. 86.1 RIA]".

Toda persona que se vea afectada por una decisión que el responsable del despliegue adopte basándose en los resultados de salida de un sistema de IA de alto riesgo que figure en el anexo III, con excepción de los sistemas enumerados en su punto 2, y que produzca efectos jurídicos o le afecte considerablemente del mismo modo, de manera que considere que tiene un efecto perjudicial para su salud, su seguridad o sus derechos fundamentales, tendrá derecho a obtener del responsable del despliegue explicaciones claras y significativas acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada [art. 86.1 RIA].

En particular, cuando el encargado del despliegue de esos sistemas sea un organismo de derecho público, o la entidad privada que preste servicios públicos, deberá realizar una evaluación de impacto de los derechos fundamentales que incluirá: a) una descripción de los procesos del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista; b) una descripción del tiempo y la frecuencia del uso del sistema de IA; c) las categorías de personas físicas y colectivos afectados; d) los riesgos del perjuicio específicos que puedan afectarles a estas personas físicas y colectivos; e) una descripción de la aplicación de medidas de supervisión humana; f) las medidas a adoptar si se materializan los riesgos. Esta obligación se aplicará al primer uso del sistema de IA de alto riesgo. En casos similares, el responsable del despliegue podrá basarse en evaluaciones de impacto relativas a los derechos fundamentales realizadas previamente o a evaluaciones de impacto existentes realizadas por los proveedores. Si, durante el uso del sistema de IA de alto riesgo, el responsable del despliegue considera que alguno de los elementos ha cambiado o ha dejado de estar actualizado, debe adoptar las medidas necesarias para actualizar la información. Si ya se cumple cualquiera de las obligaciones establecidas en este artículo mediante la evaluación de impacto relativa a la protección de datos realizada con arreglo al artículo 35 del RGPD o del artículo 27 de la Directiva (UE) 2016/680, la evaluación de impacto a la que nos referíamos complementará dicha evaluación de impacto relativa a la protección de datos. Una vez realizada

la evaluación, el responsable del despliegue debe notificar sus resultados a la autoridad de vigilancia del mercado, presentando un modelo cumplimentado que elaborará la Oficina de IA [art. 27 RIA; art. 49.3 RIA].

- Cooperar con las autoridades competentes pertinentes en cualquier medida que estas adopten en relación con el sistema de IA de alto riesgo con el objetivo de aplicar el RIA [art. 26.12 RIA].

- Las obligaciones de las AA.PP. como proveedoras de sistemas de IA:

  Las AA.PP. también pueden ser proveedoras de sistemas de IA, es decir, pueden desarrollar sistemas de IA o contratar el desarrollo de sistemas de IA, e introducirlos en el mercado o ponerlos en servicio, ya sea de forma gratuita o previo pago. En estos casos, las AA.PP. deberán cumplir con una serie de obligaciones que el RIA establece en su artículo 16 para los proveedores de sistemas de IA de alto riesgo:

  - Velar por que sus sistemas de IA de alto riesgo cumplan los requisitos definidos en la sección 2;

  - Indicar en el sistema de IA de alto riesgo o, cuando no sea posible, en el embalaje del sistema o en la documentación que lo acompañe, según proceda, su nombre, su nombre comercial registrado o marca registrada y su dirección de contacto;

  - Contar con un sistema de gestión de la calidad, en los términos del artículo 17 RIA;

  - Conservar la documentación a que se refiere el artículo 18 RIA;

  - Cuando estén bajo su control, conservar los archivos de registro generados automáticamente por sus sistemas de IA de alto riesgo a que se refiere el artículo 19;

  - Asegurarse de que los sistemas de IA de alto riesgo sean sometidos al procedimiento pertinente de evaluación de

"Las AA.PP. también pueden ser proveedoras de sistemas de IA, es decir, pueden desarrollar sistemas de IA o contratar el desarrollo de sistemas de IA, e introducirlos en el mercado o ponerlos en servicio, ya sea de forma gratuita o previo pago. En estos casos, las AA.PP. deberán cumplir con una serie de obligaciones que el RIA establece en su artículo 16 para los proveedores de sistemas de IA de alto riesgo".

la conformidad a que se refiere el artículo 43 antes de su introducción en el mercado o puesta en servicio;

- Elaborar una declaración UE de conformidad en virtud de lo dispuesto en el artículo 47;
- Colocar el marcado CE en el sistema de IA de alto riesgo o, cuando no sea posible, en su embalaje o en la documentación que lo acompañe, para indicar la conformidad con el RIA;
- Cumplir con las obligaciones de registro a que se refiere el artículo 49, apartado 1;
- Adoptar las medidas correctoras necesarias y facilitar la información exigida en el artículo 20;
- Demostrar, previa solicitud motivada de la autoridad nacional competente, la conformidad del sistema de IA de alto riesgo con los requisitos establecidos en la sección 2;
- Velar por que el sistema de IA de alto riesgo cumpla requisitos de accesibilidad de conformidad con las Directivas (UE) 2016/2102 y (UE) 2019/882.

Además, las AA.PP. proveedoras de sistemas de IA también deben registrar los sistemas de IA de alto riesgo enumerados en el Anexo III RIA en la base de datos de la UE [art. 71 RIA], establecer un sistema de vigilancia poscomercialización [art. 72 RIA]; así como notificar a las autoridades de vigilancia del mercado de cualquier incidencia grave [art. 73 RIA].

"las AA.PP. proveedoras de sistemas de IA también deben registrar los sistemas de IA de alto riesgo enumerados en el Anexo III RIA en la base de datos de la UE [art. 71 RIA], establecer un sistema de vigilancia poscomercialización [art. 72 RIA]; así como notificar a las autoridades de vigilancia del mercado de cualquier incidencia grave [art. 73 RIA]".

Por último, hacer mención de lo dispuesto en el artículo 62 RIA, que prevé una serie de medidas a tomar por los Estados miembros, en particular en las pymes y empresas emergentes, y en algún caso en las autoridades públicas locales. En el caso de las autoridades públicas locales, los Estados miembros deben adoptar las siguientes medidas: *"b) organizarán actividades de sensibilización y formación específicas sobre la aplicación del presente Reglamento adaptadas a las necesidades de las pymes, incluidas las empresas emergentes, los responsables del despliegue y, en*

su caso, las autoridades públicas locales; c) utilizarán canales específicos existentes y establecerán, en su caso, nuevos canales para la comunicación con las pymes, incluidas las empresas emergentes, los responsables del despliegue y otros agentes innovadores, así como, en su caso, las autoridades públicas locales, a fin de proporcionar asesoramiento y responder a las dudas planteadas acerca de la aplicación del presente Reglamento, también en relación con la participación en los espacios controlados de pruebas para la IA".

2.5. IA sujeta a los prinicpios y oblogaciones en proteccion de datos de carácter personal

No todas las soluciones IA tratan datos personales en alguna de las etapas de su ciclo de vida, ni toman decisiones basadas únicamente en tratamientos automatizados que afectan a personas físicas. Algunos ejemplos de soluciones IA sin datos personales podrían ser los sistemas de control de calidad de productos industriales, o aquellos sistemas de toma de decisiones sobre la compra y venta de productos financieros. No obstante, si un componente IA realiza el tratamiento de datos personales, elabora perfiles sobre una persona física o si toma decisiones sobre la misma, tendrá que someterse al RGPD.

"No todas las soluciones IA tratan datos personales en alguna de las etapas de su ciclo de vida, ni toman decisiones basadas únicamente en tratamientos automatizados que afectan a personas físicas. Algunos ejemplos de soluciones IA sin datos personales podrían ser los sistemas de control de calidad de productos industriales, o aquellos sistemas de toma de decisiones sobre la compra y venta de productos financieros".

La Agencia Española de Protección de Datos (en adelante, AEPD), en su documento de *"Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción"* (febrero de 2020) analiza aquellos aspectos clave que han de tenerse en cuenta a la hora de definir un tratamiento que haga uso de soluciones de IA para garantizar que respeta los principios establecidos en el RGPD, que extractaremos a continuación.

- **Legitimación y limitación del tratamiento:**

El establecimiento de una base jurídica legitimadora es el primer paso para determinar el cumplimiento de la solución de IA con el RGPD. La legitimación para las distintas etapas del ciclo de vida y para cada tratamiento se tiene que establecer en la fase de concepción del tratamiento, sea este

"La legitimación para las distintas etapas del ciclo de vida y para cada tratamiento se tiene que establecer en la fase de concepción del tratamiento, sea este tratamiento la propia creación de un componente IA o un tratamiento que plantee la utilización de un componente IA. Desde el punto de vista de la Protección de Datos, la legitimación es el primer elemento que hay que establecer dentro de la fase de concepción del tratamiento. Si no se encuentra una base legitimadora no se debe realizar el tratamiento".

tratamiento la propia creación de un componente IA o un tratamiento que plantee la utilización de un componente IA. Desde el punto de vista de la Protección de Datos, la legitimación es el primer elemento que hay que establecer dentro de la fase de concepción del tratamiento. Si no se encuentra una base legitimadora no se debe realizar el tratamiento.

Debido a la naturaleza de los sistemas de IA, en cada etapa del ciclo de vida se podría hacer uso de una base jurídica distinta para:

- El entrenamiento y/o validación del modelo.
- El uso de datos de terceros en la inferencia.
- La comunicación de datos implícitos en el modelo.
- El tratamiento de los datos del interesado en el marco del servicio prestado por la IA.
- El tratamiento de datos del interesado para la evolución del modelo.

El artículo 6 del RGPD establece las seis bases jurídicas por las cuales el tratamiento de datos personales se puede considerar lícito. Las bases jurídicas más habituales que legitimarán el tratamiento en una solución de IA son:

- El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte, o para la aplicación de medidas precontractuales a petición de este. Podría ser el caso de desarrolladores que contraten a sujetos para hacer uso de sus datos personales en la etapa de entrenamiento del sistema. También podría ser que el responsable del tratamiento, y que proporciona un servicio a terceros interesados que incluye la solución de IA, utilizara los datos de estos en el marco del contrato del servicio.

- El interés legítimo, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Hay que tener en cuenta que el utilizar como base jurídica el interés legítimo reclama del responsable un mayor grado compromiso, formalidad y competencia. Exige realizar una cuidadosa evaluación de que

"El interés legítimo, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Hay que tener en cuenta que el utilizar como base jurídica el interés legítimo reclama del responsable un mayor grado compromiso, formalidad y competencia".

sus intereses legítimos prevalecen sobre el posible impacto en los derechos, libertades e intereses de los interesados.

- El consentimiento de los interesados, que, como establece el artículo 4.11 del RGPD, es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. Y en ciertos casos más especiales desde el punto de vista de soluciones IA, también pueden ser bases jurídicas:
  - Protección de intereses vitales.
  - Razones de interés público o ejercicio de poderes públicos.
  - Cumplimiento de obligaciones legales.

Para determinar la base jurídica del tratamiento, es importante tener en cuenta que las categorías especiales de datos, establecidas en el artículo 9 del RGPD, tienen requisitos adicionales para su tratamiento. En estos casos, y antes de analizar una base jurídica que legitime el tratamiento según el artículo 6 del RGPD, es necesario levantar la prohibición previa establecida en el citado artículo 9 en base a alguna de las circunstancias en él contempladas, sin perder de vista las limitaciones adicionales establecidas en la LOPDGDD también en su artículo 9.

Además, el Considerando 71 del RGPD establece una restricción adicional sobre el tratamiento de las categorías especiales de datos cuando se pretendan utilizar en decisiones automatizadas y para la elaboración de perfiles, fijando la limitación de que estos solo pueden ser empleados bajo condiciones específicas. En particular, el artículo 22.4 establece que las decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en el interesado o le afecte significativamente de modo similar, no se basarán en las categorías especiales de datos personales salvo que medie el consentimiento del interesado o el tratamiento sea

necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. Estas limitaciones aplican tanto a los datos recogidos de los interesados para el desarrollo o explotación del componente de IA, como a las categorías especiales de datos que se infieran en el curso de los tratamientos.

Otro aspecto importante es que se debe tener en cuenta el principio de limitación del tratamiento. Una base jurídica no habilita para el uso de los datos para cualquier propósito y en todo momento, sino que debe restringirse a aquellos fines determinados, explícitos y legítimos que se hayan identificado, evitando tratarlos de manera incompatible con esos fines. Además, los interesados cuyos datos son tratados, deben ser conscientes de cómo se van a utilizar, lo que está íntimamente relacionado con el principio de información y transparencia.

"Otro aspecto importante es que se debe tener en cuenta el principio de limitación del tratamiento. Una base jurídica no habilita para el uso de los datos para cualquier propósito y en todo momento, sino que debe restringirse a aquellos fines determinados, explícitos y legítimos que se hayan identificado, evitando tratarlos de manera incompatible con esos fines".

La extinción de una base jurídica de legitimación, como puede ser la retirada del consentimiento, no tiene un efecto retroactivo con relación a los resultados obtenidos en un tratamiento ya realizado. Por ejemplo, cuando los datos personales se han empleado para entrenar un componente de IA, la extinción de la base jurídica no invalida la explotación del modelo, aunque el responsable del tratamiento ha de prestar atención a las solicitudes del ejercicio de derechos en materia de protección de datos.

- **Información y transparencia:**

La información que cada responsable ha de proporcionar a los interesados se establece en los artículos 13 y 14 del RGPD, y el contenido concreto se tendrá que adaptar a la etapa del ciclo de vida de la IA en la que se esté realizando el tratamiento.

En el caso de que en el componente IA existan datos personales que puedan ser recuperables hay que informar sobre dicha circunstancia a los interesados y, en su caso,

disponer de una base jurídica legitimadora para su comunicación o tratamiento posterior.

En el caso de que el interesado esté sometido a decisiones automatizadas o en la elaboración de perfiles a los que hace referencia el artículo 22 del RGPD, un aspecto importante que se establece en el artículo 13.2.f del RGPD es que éste ha de "disponer de información significativa sobre la lógica aplicada" y "la importancia y las consecuencias previstas". A juicio de la AEPD, cumplir con esta obligación ofreciendo una referencia técnica a la implementación del algoritmo puede ser opaco, confuso, e incluso conducir a la fatiga informativa, por lo que debe facilitarse información que permita entender el comportamiento del tratamiento.

Si vamos al RIA, encontramos que su artículo 13 establece que los sistemas de alto riesgo deben diseñarse y desarrollarse de forma que se garantice un nivel de transparencia suficiente para que los responsables del despliegue interpreten y utilicen correctamente sus resultados de salida e, igualmente, puedan cumplir las obligaciones previstas en la sección 3 (artículos 16 a 27). También se establece que los sistemas de IA de alto riesgo deberán ir acompañados de instrucciones de uso, que deberán incluir información concisa, completa, correcta y clara, que sea pertinente, accesible y comprensible por los responsables del despliegue (ap. 2). El apartado 3 fija el contenido mínimo de las instrucciones de uso. La Autoridad Catalana de Protección de Datos (en adelante, APDCAT) en el documento *"RGPD vs. RIA Análisis de una intersección parcial"* (julio de 2024), destaca de este contenido lo siguiente: el nivel de precisión, solidez y ciberseguridad; los eventuales riesgos que puedan aparecer y afectar a la salud y a la seguridad o a los derechos fundamentales (en conexión con el EIDDFF del artículo 27); las especificaciones relativas a los datos de entrada o cualquier información relevante sobre el conjunto de datos de entrenamiento, validación y prueba empleados, teniendo en cuenta la finalidad del sistema; cualquier información que permita interpretar los resultados de salida a los responsables del despliegue, así como utilizarla correctamente; y, una descripción de los mecanismos incluidos en el sistema que permita a los

"La información que cada responsable ha de proporcionar a los interesados se establece en los artículos 13 y 14 del RGPD, y el contenido concreto se tendrá que adaptar a la etapa del ciclo de vida de la IA en la que se esté realizando el tratamiento".

"Este articulo prevé que los proveedores deberán garantizar que los sistemas de IA que se destinen a interactuar con personas físicas deben diseñarse y desarrollar de manera que las personas físicas que intervienen estén informadas de que están interactuando con un sistema de inteligencia artificial. Esto no se aplicará cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz; ni cuando los sistemas de IA se destinen a detectar, prevenir, investigar o enjuiciar delitos (ap. 1)".

responsables obtener, almacenar e interpretar correctamente los archivos de registro (artículo 12 RIA). Toda esta información, según la APDCAT, servirá también a los efectos de cumplir con las obligaciones de transparencia e información del RGPD cuando los sistemas de IA traten datos personales.

Esto, sin embargo, no debe confundirse con lo que dispone el artículo 50 RIA, que versa sobre las obligaciones de transparencia de los proveedores o responsables del despliegue hacia las personas físicas. Concretamente, este artículo prevé que los proveedores deberán garantizar que los sistemas de IA que se destinen a interactuar con personas físicas deben diseñarse y desarrollar de manera que las personas físicas que intervienen estén informadas de que están interactuando con un sistema de inteligencia artificial. Esto no se aplicará cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz; ni cuando los sistemas de IA se destinen a detectar, prevenir, investigar o enjuiciar delitos (ap. 1). Las personas físicas deberán ser informadas de manera clara y distinguible, y no más tarde de la primera interacción o exposición al sistema de IA (ap. 5).

- **Ejercicio de derechos:**

Los responsables que hagan uso de soluciones de IA para tratar datos personales, elaborar perfiles o tomar decisiones automatizadas, han de ser conscientes de que los interesados tienen derechos en el ámbito de la protección de datos que deben ser atendidos. Por lo tanto, durante la fase de concepción del tratamiento, los responsables han de ser conscientes de que tienen que establecer mecanismos y procedimientos adecuados para poder atender las solicitudes que reciban, y que dichos mecanismos deberán estar adecuadamente dimensionados para la escala del tratamiento que están efectuando.

- **Derecho de acceso**: El derecho de acceso ha de ejecutarse por el responsable de cada una de las etapas del ciclo de vida de la solución de IA que involucren datos de

carácter personal. Esto incluye los datos de entrenamiento que pudieran estar incluidos en los componentes de IA y que puedan ser recuperados por el responsable que explota la solución IA.

- **Derecho de supresión**: El derecho de supresión implica una proactividad del responsable del tratamiento para, como establece el Considerando 39, garantizar que los datos se suprimen cuando ya no sean necesarios para la finalidad del tratamiento y, en particular, para que se incluyan procedimientos para la revisión periódica del conjunto de datos y plazos para su supresión.

Los datos recogidos para la etapa de entrenamiento, atendiendo a lo señalado en relación con el artículo 11 del RGPD y en cumplimiento del principio de minimización de datos, han de ser depurados de toda la información no estrictamente necesaria para el entrenamiento del modelo.

Cuando la etapa de entrenamiento del sistema de IA se ha completado, la organización ha de ejecutar su supresión, a menos que se justifique la necesidad de mantenerlos para el refinado o evaluación del sistema, o se justifique la necesidad y legitimidad de mantenerlos para otras finalidades que resulten compatibles con las que originaron su recogida de acuerdo con las condiciones del artículo 6.466 del RGPD y aplicando los principios de minimización de datos. En el caso de que se reciban solicitudes de supresión de los interesados, el responsable tendría que adoptar una aproximación caso por caso, teniendo en cuenta las posibles limitaciones a este derecho previstas en el Reglamento.

En el caso de que el responsable mantenga los datos del interesado para la personalización del servicio que está ofreciendo la solución de IA, una vez haya extinguido la relación de servicio, estos datos deberán de ser suprimidos.

- **Derecho de rectificación**: El responsable tiene la obligación de atender el derecho de rectificación de los datos de los interesados, especialmente aquellos generados por las inferencias y perfiles elaborados por la solución IA.

"Los datos recogidos para la etapa de entrenamiento, atendiendo a lo señalado en relación con el artículo 11 del RGPD y en cumplimiento del principio de minimización de datos, han de ser depurados de toda la información no estrictamente necesaria para el entrenamiento del modelo".

"En la medida que existan datos inexactos de entrenamiento en el modelo que no tengan un efecto sobre el interesado, por ejemplo, que no haya una posible vinculación de la información inexacta con algún interesado a la hora de distribuir la solución de IA, la inexactitud en los datos puede ser aconsejable como parte de las estrategias de abstracción y ocultación encaminadas a garantizar la aplicación del principio de minimización".

Por otro lado, en la medida que existan datos inexactos de entrenamiento en el modelo que no tengan un efecto sobre el interesado, por ejemplo, que no haya una posible vinculación de la información inexacta con algún interesado a la hora de distribuir la solución de IA, la inexactitud en los datos puede ser aconsejable como parte de las estrategias de abstracción y ocultación encaminadas a garantizar la aplicación del principio de minimización. Si dichas estrategias conducen a evitar la reidentificación de individuo, haciendo referencia al artículo 11 del RGPD antes citado, no cabría la ejecución del derecho de rectificación.

Por el contrario, si el modelo en sí contiene datos personales inexactos de terceros que pueden ser reidentificados, asociando a dicho terceros una información errónea, es necesario dar respuesta al derecho de rectificación.

- **Portabilidad**: El responsable de un tratamiento que incluya un componente de IA ha de evaluar y documentar si su tratamiento está obligado a proporcionar la portabilidad sobre los datos facilitados u observados del interesado, en función de lo establecido en el artículo 20 antes citado. En ese caso, el requisito de portabilidad ha de ser tenido en cuenta desde las más tempranas fases de concepción y diseño del tratamiento, en la selección del componente IA y/o por los desarrolladores de componentes IA.

El artículo 20.2 del RGPD establece el derecho a la transmisión de los datos directamente de responsable a responsable, pero sólo cuando sea técnicamente posible. En caso de que existan limitaciones a la portabilidad, es un ejercicio de transparencia informar con antelación a los usuarios de dichas limitaciones.

- **Toma de decisiones basadas únicamente en un tratamiento automatizado:**

Las aplicaciones que ofrecen o soportan un servicio basado en soluciones IA pueden tomar decisiones que afectan a los individuos, sus vidas privadas, su seguridad física, su posición social y su interacción con otras personas. El RGPD garantiza el derecho a no ser sometido a decisiones automatizadas incluidas la elaboración de perfiles cuando:

"Más allá de exigencias derivadas de la protección de datos, como buena práctica, la AEPD aboga por la supervisión humana en IA, y en general, en la toma decisiones automatizadas, dando siempre la opción de que un operador humano pueda ignorar el algoritmo en un momento dado, procedimentando aquellas situaciones en las que debe optarse por este modo de actuar".

- No hay intervención humana. Para que pueda considerarse que existe participación humana, la supervisión de la decisión ha de ser realizada por una persona competente y autorizada para modificar la decisión, y para ello ha de realizar una acción significativa y no simbólica.
- Produzcan efectos jurídicos.
- afecte de forma similar y significativa al interesado

Si bien, el RGPD lo permite en una serie de circunstancias [art. 22.2 RGPD]. En estos casos, habrá que atender a lo dispuesto en el apartado "Información" antes tratado se trata sobre los requisitos de información de estos tratamientos.

Más allá de exigencias derivadas de la protección de datos, como buena práctica, la AEPD aboga por la supervisión humana en IA, y en general, en la toma decisiones automatizadas, dando siempre la opción de que un operador humano pueda ignorar el algoritmo en un momento dado, procedimentando aquellas situaciones en las que debe optarse por este modo de actuar. Para ello es recomendable documentar las incidencias o los cuestionamientos de las decisiones automáticas recibidas de los interesados, de modo que, de su análisis, sea posible detectar situaciones en las que es necesaria la intervención humana porque el tratamiento puede no estar funcionando de la manera esperada.

El RIA, por su parte, no crea ni prevé ninguna figura específica para realizar las tareas de supervisión o vigilancia de los sistemas de IA. Sin embargo, el considerando 73 y el artículo 26.2 (obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo) establecen que los responsables del despliegue encargarán la supervisión humana de los sistemas a personas físicas que tengan la competencia, la formación y la autoridad necesarias.

- **Gestión del riesgo para los derechos y libertades:**

El RGPD establece en su artículo 32 que tanto el responsable, como el encargado, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de

seguridad adecuado al riesgo para los derechos y libertades de los interesados. Estas medidas se adecuarán a los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como a los riesgos de probabilidad y gravedad variables. Es decir, no hay una solución estándar para todos los tratamientos, y mucho menos para aquellos que incluyan un componente de IA. La solución tiene que establecerse mediante un análisis de riesgos que, desde el punto de vista de protección de datos, ha de ser relativo a los riesgos para los derechos y libertades de los interesados.

El responsable del desarrollo, mantenimiento y/o distribución de un componente IA, así como el responsable de un tratamiento que incluya componentes IA, ha de tomar, en cada una de las respectivas etapas y responsabilidades, las medidas oportunas para minimizar o eliminar los factores de riesgo.

"No hay una solución estándar para todos los tratamientos, y mucho menos para aquellos que incluyan un componente de IA. La solución tiene que establecerse mediante un análisis de riesgos que, desde el punto de vista de protección de datos, ha de ser relativo a los riesgos para los derechos y libertades de los interesados".

- **Evaluación de Impacto en Protección de Datos (EIPD):**

La EIPD es una obligación establecida en el RGPD cuando los niveles de riesgo asociados al tratamiento son elevados. Esta obligación implica ir más allá de realizar la mera gestión del riesgo del tratamiento, puesto que exige una formalidad adicional a la hora de ejecutar dicha gestión.

La necesidad de que cada responsable lleve a cabo una evaluación de impacto de la protección de datos se establece en el artículo 35 del RGPD cuando, según el apartado 1, "el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas". En particular, pero no de forma exclusiva, y tal como establece el artículo 35.3.a), es necesario realizar una EIPD cuando se realice la elaboración de perfiles, basados en tratamientos automatizados (pero no necesariamente exclusivamente automatizados), sobre los que se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente.

Como veíamos en el apartado de "Obligaciones y responsabilidades de los entes del sector público", en el RIA se incorporan varias referencias a las EIPD reguladas por la

"Es necesario realizar una EIPD cuando se realice la elaboración de perfiles, basados en tratamientos automatizados (pero no necesariamente exclusivamente automatizados), sobre los que se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente".

normativa de protección de datos. Entre las más significativas:

- La del artículo 26.9 RIA, que establece que, cuando proceda, los responsables del despliegue de sistemas de IA de alto riesgo deben utilizar la información facilitada conforme al artículo 13 del RIA (transparencia y comunicación de información) para cumplir la obligación de llevar a cabo una evaluación de impacto relativa a la protección de datos que les imponen el artículo 35 del Reglamento (UE) 2016/679 o el artículo 27 de la Directiva (UE) 2016/680.

- La del artículo 27 RIA, que señala que antes de desplegar uno de los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, con excepción de los sistemas de IA de alto riesgo destinados a ser utilizados en el ámbito enumerado en el anexo III, punto 2, los responsables del despliegue que sean organismos de Derecho público, o entidades privadas que prestan servicios públicos, y los responsable del despliegue de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, letras b) y c), llevarán a cabo una evaluación del impacto que la utilización de dichos sistemas puede tener en los derechos fundamentales. Ahora bien, en su apartado 4, este artículo precisa que si ya se cumple esa obligación mediante la EIPD realizada con arreglo al artículo 35 RGPD o 27 de la Directiva (UE) 2016/680, la evaluación de impacto relativa a los derechos fundamentales a que se refiere el artículo 27 complementará dicha evaluación de impacto relativa a la protección de datos.

En lo que respecta a la obligación de hacer pública o no la EIPD en el ámbito de los sistemas de IA de alto riesgo, nos remitimos a lo dispuesto por la APDCAT en el documento *"RGPD vs. RIA Análisis de una intersección parcial"*, y es que, si nos limitamos al ámbito del RGPD, no es obligatorio dar publicidad a la misma. No obstante, según las directrices del Grupo de Trabajo del artículo 29 (ahora, Comité Europeo de Protección de Datos), su publicación podría ayudar a fomentar la confianza en el tratamiento de los datos y demostrar responsabilidad proactiva y transparencia. En este sentido, se apuntaba que sería positivo publicar algunas partes o un resumen de la misma. En el RIA, en cambio,

artículo 49.3 y 4, se prescribe que antes de poner en servicio o utilizar un sistema de IA de alto riesgo del listado del anexo III, con excepción de los del apartado 2 (infraestructuras críticas), los responsables del despliegue de los sistemas de IA de alto riesgo que sean autoridades públicas, instituciones, órganos u organismos de la Unión, o personas que actúen en su nombre, se deben registrar, seleccionar el sistema y registrar su uso en la base de datos del artículo 71. Por tanto, las AA.PP. responsables del despliegue deberán aportar para dicha inscripción un resumen de la EIPD, que se hará público y accesible para todos, antes de utilizar un sistema de IA de alto riesgo del anexo III (excluyendo los sistemas de los puntos 1, 2, 6 y 7).

"Por tanto, las AA.PP. responsables del despliegue deberán aportar para dicha inscripción un resumen de la EIPD, que se hará público y accesible para todos, antes de utilizar un sistema de IA de alto riesgo del anexo III (excluyendo los sistemas de los puntos 1, 2, 6 y 7)".

- **Minimización:**

Se ha de garantizar que los datos personales son adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Consiste en:

- Limitar la extensión de las categorías de datos98 que se utilizan en cada fase del tratamiento a aquellas que son estrictamente necesarias y relevantes.
- Limitar el grado de detalle o precisión de la información99, la granularidad de la recogida en tiempo y frecuencia y la antigüedad de la información utilizada.
- Limitar la extensión en el número de interesados de los que se tratan los datos.
- Limitar la accesibilidad de las distintas categorías de datos al personal del responsable/encargado o incluso al usuario final (si hay datos de terceros en los modelos de IA) en todas las fases del tratamiento.

Es necesario que en la concepción de la solución IA se estudie la forma de implementar estas restricciones, describiendo y analizando el ciclo de vida de los datos a lo largo de todas las etapas del tratamiento. El análisis no puede centrarse únicamente en la solución IA desde el punto de vista técnico, sino que debe englobar todo el tratamiento en el que se incluye y alcanzando tanto los aspectos automatizados como los no automatizados de todas y cada una de las fases del tratamiento.

"Uno de los aspectos claves del RGPD, y capital para determinar la correcta aplicación de las políticas de accountability y transparencia, es que estén claramente identificadas las responsabilidades en el tratamiento".

- **Roles y responsabilidades en materia de protección de datos:**

Uno de los aspectos claves del RGPD, y capital para determinar la correcta aplicación de las políticas de *accountability* y transparencia, es que estén claramente identificadas las responsabilidades en el tratamiento.

En las distintas etapas del ciclo de vida de un componente IA será responsable del tratamiento de datos personales aquella persona física, jurídica, autoridad pública u otro que tome la decisión de realizar el tratamiento de datos personales. Por lo tanto, distintas responsabilidades implicarán distintas obligaciones en el marco del tratamiento. Es posible que el responsable contrate a terceras partes para realizar, en su nombre y bajo sus instrucciones, diferentes tareas. Dichos terceros tendrán el carácter de encargados de tratamiento siempre y cuando todo tratamiento de datos personales lo realicen bajo las instrucciones de ese responsable. Cualquier otro tratamiento adicional sobre dichos datos que puedan llegar a realizar para sus propios fines los convertirá en responsables para esos tratamientos.

Asimismo, en las distintas etapas pueden intervenir distintos responsables y encargados, además de plantearse situaciones de comunicaciones de datos entre responsables:

Etapa	Responsable	Encargado
Desarrollo/ Entrenamiento	La entidad que defina los fines del componente IA y decida qué datos se van a emplear para entrenar el sistema. En caso de que se contrate el desarrollo a un tercero, pero este tercero tome las decisiones sobre los datos personales utilizados para entrenar al componente IA para sus propios fines, será considerado responsable la entidad contratada. En el caso que, aquel que defina los fines, adquiera un conjunto de datos personales, será responsable de tratamiento.	La entidad contratada, para entrenamiento o desarrollo, siempre y cuando el contratante fije los términos que definen los fines del tratamiento y las características sustanciales de los datos, tanto si el contratante es quien cede dichos datos como si los obtiene por sí mismo el contratado, y el encargado los utilice sólo para cumplir con los fines del responsable.
Validación	Igual que en el caso anterior.	Igual que en el caso anterior.
Despliegue	En el caso de que la solución IA es un componente que se vende a otra entidad (podría ser formando parte de tratamiento), y ese componente incluye datos de carácter personal, ambas entidades realizan una comunicación de datos personales y ambas son responsables. Si la comercialización tiene como objeto la venta de un producto que incluya un componente de IA a una persona física para su uso particular, aunque el modelo incluya datos de carácter personal, aplicará la excepción doméstica, salvo que realice un tratamiento para sus propios fines de los datos personales incluidos, en cuyo caso también será considerado responsable.	La entidad que pone un modelo al servicio de un responsable para que lo explote en un marco de prestación de servicios sin intervenir en esa explotación o que, en caso de hacerlo porque sea necesario para la adecuada ejecución de ese servicio, no utiliza los datos personales para fines propios.

Inferencia/perfilado	La entidad que decide tratar los datos de los interesados con el sistema IA para sus propios fines. Si el tratamiento lo realiza una persona física sobre sus propios datos personales o de aquellas personas en su entorno para una actividad exclusivamente personal o doméstica, se aplicará la excepción doméstica. Esta excepción no aplica a aquellos que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas53 para sus propios fines.	Igual que en el caso anterior.
Decisión	La entidad que tome decisiones automatizadas sobre los interesados para sus propios fines.	Igual que en el caso anterior.
Evolución	La entidad que decide tratar los datos de los interesados con el sistema IA, si comunica a una tercera entidad los datos de los usuarios será responsable de la comunicación de datos si no existe una relación de responsable-encargado. La entidad que determina la evolución del componente IA en base a los datos de los usuarios, tanto si los datos son cedidos directamente por los interesados como por la entidad que les proporciona servicio, es responsable de dicho tratamiento de evolución o reentrenamiento.	En el caso que la entidad que decide tratar los datos de los interesados contrate el tratamiento IA a un tercero, dicho tercero actuará como encargado de tratamiento, siempre que no los trate para sus propios fines.

"El que toma la decisión de realizar el tratamiento es responsable, y no puede escudarse en la carencia de información o el desconocimiento técnico para evadir su responsabilidad a la hora de auditar y decidir la adecuación del sistema."

Matizar que en este apartado se está tratando el tema de responsabilidad desde el punto de vista de protección de datos. La decisión de adoptar, en el marco de un tratamiento, una solución técnica basada en IA, es tomada por el responsable, que es quien "determina los medios y fines del tratamiento" y es, por tanto, quien tiene a su cargo la toma de decisión de seleccionar una solución tecnológica u otra. En dicho responsable descansa la obligación de ser diligente a la hora de seleccionar la más adecuada, en particular cuando contrata su desarrollo o la adquiere; exigir y analizar las especificaciones de calidad de la solución; y determinar la extensión del tratamiento y la carga de hacer frente a las consecuencias de sus decisiones. El que toma la decisión de realizar el tratamiento es responsable, y no puede escudarse en la carencia de información o el desconocimiento técnico para evadir su responsabilidad a la hora de auditar y decidir la adecuación del sistema.

- **Delegado de Protección de Datos:**

El DPD podrá orientar la implementación de las políticas de transparencia, en particular, para gestionar un canal de información a los interesados. El DPD se convierte en un elemento clave para poder gestionar el riesgo y aplicar de forma efectiva los mecanismos de responsabilidad proactiva. En particular, el artículo 35 identifica al DPD como un rol fundamental en la realización de la EIPD y una de las herramientas para implementar la transparencia de cara al usuario.

MATERIAL COMPLEMENTARIO

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).
  Consulta en este este enlace.

- Guía de la AEPD; Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. Consulta la guía en este enlace.

- Artículo de interés, Víctor Almonacid; *Smart City 2024: ejemplos de #IA aplicada a los servicios municipales*. Consulta el artículo en este enlace.

- Marco de roles y responsabilidades para IA en infraestructuras críticas del Departamento de Seguridad Nacional de EEUU. Consulta en este enlace.

NOTICIAS

Las autoridades de control en protección de datos españolas han publicado varias noticias, de interés general:

1. **La Autoridad Italiana de Protección de Datos adopta medidas correctivas y sancionadoras contra OpenAI por el uso de ChatGPT**

La Autoridad de Protección de Datos italiana multó a OpenAI con 15 millones de euros por varias infracciones relacionadas con el procesamiento de datos personales de ChatGPT. La investigación de 2023 reveló que OpenAI no notificó una violación de datos, procesó información sin base legal y no cumplió con las obligaciones de transparencia. Además, no implementó controles de edad, exponiendo a menores de 13 años a riesgos. OpenAI deberá realizar una campaña informativa de seis meses sobre el funcionamiento de ChatGPT. Puedes consultar la Resolución en este enlace.

2. **El Comité Europeo de Protección de Datos (CEPD) emite un Dictamen sobre los modelos de IA: los principios del RGPD respaldan la IA responsable**

El CEPD aprobó un dictamen sobre el uso de datos personales en modelos de IA, abordando la anonimización, el interés legítimo como base jurídica y el tratamiento ilegal de datos. Establece que las Autoridades de Protección de Datos deben evaluar caso por caso si un modelo es anónimo y si el interés legítimo es adecuado, asegurando que el tratamiento sea necesario y respetuoso con los derechos. También se señala que el uso de datos personales tratados ilegalmente puede afectar la legalidad del modelo, a menos que se haya anonimizado. Además, el CEPD prepara directrices sobre temas como el raspado de páginas web. Puedes consultar el Dictamen 28/2024 en este enlace.