



OBSERVACIONES DEL CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS AL “ANTEPROYECTO DE LEY DE ADMINISTRACIÓN DIGITAL E INTELIGENCIA ARTIFICIAL DE LA COMUNIDAD DE MADRID”.

Con fecha 10 de febrero de 2026 se ha recibido en este Consejo un escrito del Director General de Estrategia Digital en el que se remite el texto del “Anteproyecto de Ley de Administración Digital e Inteligencia Artificial de la Comunidad de Madrid” junto con la memoria de análisis de impacto normativo, solicitando que se emita el correspondiente informe, de conformidad con lo dispuesto en el artículo 4.2.o) del reglamento de organización y funcionamiento del Consejo de Transparencia y protección de Datos de la Comunidad de Madrid.

Se realizan las siguientes observaciones al articulado del Anteproyecto:

- a) **Artículo 3 Definiciones. c):** Se sugiere sustituir la definición de “Datos neuronales: datos personales biométricos derivados de la actividad del sistema nervioso.” por la siguiente: “Datos neuronales: Datos personales de categoría especial obtenidos del sistema nervioso mediante tecnologías capaces de interpretar o interactuar con la actividad cerebral. Son datos personales cuyo tratamiento está prohibido salvo que concurra alguna de las circunstancias indicadas en el artículo 9.2 del Reglamento General de Protección de Datos.”

Justificación: Parte del texto sugerido se corresponde con la definición utilizada por la Agencia Española de Protección de Datos para los neurodatos.

- b) **Artículo 3 Definiciones. n):** Se sugiere mejorar la definición, sustituyendo “Trazabilidad de los datos: característica de los datos que permite conocer el proceso que han seguido desde su inicio.” por la siguiente: “Trazabilidad de datos: Capacidad de rastrear el origen, transformación, movimiento y uso de los datos a lo largo de todo su ciclo de vida.”
- c) **Artículo 3 Definiciones, en general:** Se sugiere añadir las definiciones del Reglamento de Inteligencia Artificial de los conceptos que se citan en esta ley y que no están incluidos en este artículo, como “datos biométricos”, “riesgo”, “entrenamiento” o “validación”.
- d) **Artículo 4 Fines. i):** Se sugiere añadir “la protección de datos personales”, quedando redactado como sigue: “Poner en marcha medidas y soluciones digitales que posibiliten el gobierno y la calidad del dato y la mayor apertura de datos posible en poder de la Administración de la Comunidad de Madrid, de acuerdo con los principios de transparencia, publicidad activa, gobierno abierto y protección de datos personales y, en general, la innovación y los nuevos servicios públicos basados en datos.”

Justificación: Las medidas y soluciones digitales que se adopten, deben de cumplir y estar de acuerdo, además de con los principios de transparencia, publicidad activa y gobierno abierto, con los principios de protección de datos personales. La protección de datos personales es un derecho fundamental al que se debe hacer referencia cuando se tratan datos.

- e) **Artículo 4 Fines. k):** Se indica lo siguiente: “Usar de manera compartida los datos para aumentar la efectividad y la confianza en el proceso de elaboración, desarrollo y ejecución de políticas e iniciativas públicas, garantizando el acceso legítimo y la reutilización de los activos de datos en el ámbito de la Comunidad de Madrid. Tal acceso y reutilización se llevará a cabo siempre dentro del máximo respeto a los principios reguladores de los datos personales y la seguridad de la información.”

Respecto a este apartado:

Se sugiere revisar el contenido y la redacción, pues entra en conflicto con el cumplimiento de la normativa de protección de datos personales tal y como se encuentra configurado su cumplimiento en la Comunidad de Madrid.

Conforme se establece en los decretos de estructura de las Consejerías de la Comunidad de Madrid, “Los diferentes centros directivos de la Consejería son responsables del tratamiento de los datos personales en su respectivo ámbito de actividad, y les corresponde la gestión, coordinación y dirección del tratamiento de los datos, así como la determinación de los fines y medios para garantizar el cumplimiento de la normativa en materia de protección de datos.”. Con esta estructura se han desarrollado e implementado todas las actuaciones de las que son responsables de tratamiento los distintos centros directivos, como la publicación de su registro de actividades de tratamiento (RAT), los procedimientos de ejercicio de derechos, los análisis o evaluaciones de riesgos en datos personales o la comunicación (cesión) de datos personales.

Lo que se establece en esta letra k) es una comunicación masiva de datos entre distintos órganos de la Administración de la Comunidad de Madrid, cuando la comunicación de datos ha de regirse por lo previsto en el Reglamento General de Protección de Datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como lo que establece el artículo 155 de la Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público. Según esta normativa, no cabe el acceso masivo o indiscriminado a datos personales. La comunicación de datos entre distintos responsables del tratamiento debe respetar el derecho a la protección de datos de las personas físicas, por lo que es necesario considerar cada caso concreto para esa comunicación de datos.

El “Usar de manera compartida los datos para aumentar la efectividad...” supondría, además, que todos los responsables de tratamiento de la Comunidad de Madrid se convirtieran en responsables de tratamiento de todos los datos personales que trata la Comunidad de Madrid con las implicaciones que acarrearía ser “responsables” de datos que realmente no tratan.

- f) **Artículo 7 Oficina Técnica de Impulso de la Inteligencia Artificial. 2, en su cuarto quion:** Se sugiere sustituir “Realizar la evaluación de los sistemas que no tengan la consideración de alto impacto” por lo siguiente “Realizar la evaluación de impacto en derechos fundamentales de los sistemas que no tengan la consideración de alto riesgo”.

Justificación: Es preciso distinguir que se trata de la evaluación de impacto sobre derechos fundamentales, que el RIA establece como obligatoria para los sistemas de alto riesgo incluidos en su Anexo III (que no de alto impacto), de la evaluación de impacto en protección de datos personales a la que obliga el RGPD cuando el sistema trata datos personales.

- g) **Artículo 9 Comité de Ética en Inteligencia Artificial. 2:** Se sugiere sustituir “...las evaluaciones de impacto algorítmico realizadas para los sistemas de alto impacto...” por lo siguiente “...las evaluaciones de impacto algorítmico realizadas para los sistemas de alto riesgo ...”.

Justificación: El RIA establece como obligatoria la evaluación de impacto sobre derechos fundamentales para los sistemas de alto riesgo incluidos en su Anexo III, no para los sistemas de alto impacto.

- h) **Artículo 13 Servicios públicos digitales. 4:** Se sugiere añadir “que garanticen la protección de datos personales”, quedando el texto redactado como sigue: “...A tal efecto, se establecerán modelos proactivos de gestión que permitan la actuación de oficio de la Administración para anticiparse a las necesidades de las personas y entidades interesadas, utilizando tecnologías como la inteligencia artificial y desarrollando una estrategia integral del dato público, basada en un modelo robusto de gobierno del dato, que garanticen la protección de datos personales.”

Justificación: El uso de la inteligencia artificial debe permitirse solo cuando haya superado las correspondientes evaluaciones de impacto, debido a los riesgos que implica su uso en el derecho a la protección de datos personales. Además, hay que tener en cuenta, en el uso de la inteligencia artificial, el cumplimiento del artículo 22 del Reglamento General de Protección de Datos, referido a las decisiones individuales automatizadas, incluida la elaboración de perfiles.

- i) **Artículo 15 Sistema de información digital compartido:** En este artículo se establece un modelo de tratamiento que implica la compartición de todos los datos, incluidos los personales, que tratan todos los centros directivos de la Comunidad de Madrid y que son responsabilidad de los mismos conforme a la normativa de protección de datos personales.

Como ya se ha comentado en el apartado referido al artículo 4.k), este modelo entra en conflicto con el cumplimiento de la normativa de protección de datos personales tal y como se encuentra configurado dicho cumplimiento en la Comunidad de Madrid. Según se establece en los decretos de estructura de las Consejerías de la Comunidad de Madrid, “Los diferentes centros directivos de la

Consejería son responsables del tratamiento de los datos personales en su respectivo ámbito de actividad, y les corresponde la gestión, coordinación y dirección del tratamiento de los datos, así como la determinación de los fines y medios para garantizar el cumplimiento de la normativa en materia de protección de datos”.

Lo que establece este artículo implica una comunicación masiva de datos entre los distintos órganos de la Administración de la Comunidad de Madrid, cuando la comunicación de datos personales ha de regirse por lo previsto en el Reglamento General de Protección de Datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, así como lo que establece el artículo 155 de la Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público.

El “conectar los conjuntos de datos o los sistemas de información con el fin de facilitar su acceso y aprovechamiento transversal o su reutilización” supondría que todos los responsables de tratamiento de la Comunidad de Madrid se convirtieran en responsables de tratamiento de todos los datos personales que trata la Comunidad, con las implicaciones que conllevaría ser responsables de datos que realmente no tratan.

Por ello se sugiere revisar la redacción de este artículo considerando al menos la inclusión de un punto final en el que se indique, para los datos personales:

- El organismo responsable del tratamiento, conforme a la normativa de protección de datos personales, tal y como se hizo con Cuenta Digital, cuyo responsable del tratamiento es la Dirección General de Estrategia Digital.
- El tratamiento o comunicación masiva de datos personales conllevará la previa anonimización de los datos personales.

j) **Artículo 16 Gobierno y gestión de datos:** Aunque el punto 3 de este artículo señala que “las herramientas digitales deberán cumplir con principios de privacidad desde el diseño, interoperatividad y evaluación de riesgos durante todo su ciclo de vida”, el indicar que “los datos tratados por los responsables en el ejercicio de funciones públicas tienen carácter institucional y común”, o que “la compartición de datos entre los distintos responsables será obligatoria por defecto”, tiene difícil encuadre en el cumplimiento de la normativa de protección de datos. Por ello se sugiere:

- Valorar en el punto 5 la modificación de redacción de: “Los datos no tendrán la consideración de propiedad exclusiva de los centros directivos.” pues la propiedad del dato personal es solo de la persona, siendo los centros directivos solo responsables de su tratamiento y a los que obliga, entre otros, el principio de confidencialidad de los datos que tratan en el ejercicio de sus funciones, conforme al RGPD.

- Valorar el incluir algún apartado que aluda a la compartición específica de los datos personales cumpliendo los requisitos que se establecen en la normativa respecto a esta comunicación de información.
- Valorar la supresión del apartado c) del punto 6, por el que se indica que “La compartición de datos por los centros directivos será obligatoria por defecto cuando resulte necesaria para el desarrollo, entrenamiento, validación o funcionamiento de sistemas o agentes de inteligencia artificial de uso público”, teniendo en cuenta los altos riesgos sobre la privacidad que tienen los tratamientos de desarrollo, entrenamiento y validación con datos personales reales.
- Valorar hacer mención, en el punto 7, a la necesaria anonimización de los datos personales antes de integrarse en los espacios de datos citados.

k) **Artículo 21 La inteligencia artificial en los servicios públicos digitales.1. a):**

Señala que “(En el uso de la inteligencia artificial se garantizarán) los derechos y libertades de los interesados, cumpliendo con lo dispuesto en la normativa reguladora de la protección de datos de carácter personal y de la inteligencia artificial, estando prohibida toda forma de manipulación no consentida de procesos cognitivos y emocionales.”

Se sugiere cambiar la redacción, y que no se haga referencia exclusiva a la prohibición del tratamiento de datos no consentido de procesos cognitivos y emocionales, pues la prohibición del tratamiento de datos personales, independientemente de que sea con inteligencia artificial o no, aplica a todos los datos personales de categorías especiales, no solo a los neurodatos. En todo caso, si se quieren tratar datos de categorías especiales, deberá concurrir alguna de las circunstancias de artículo 9.2 del RGPD.

Se sugiere también tener en cuenta el artículo 22 del RGPD en la redacción de este apartado que establece que todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o que afecte significativamente de modo similar. Esto no se aplicará si ha dado su consentimiento o el responsable ha tomado las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado lo que parece estar implícito en el texto de la ley. En el modelo que se propone de uso de inteligencia artificial de “datos compartidos”, tiene difícil encaje la ejecución efectiva, por parte del responsable del tratamiento, de los derechos que tiene un ciudadano si este solicita el derecho a la supresión de sus datos o el derecho a no ser objeto de decisiones automatizadas o a que no se le profile.

- l) **Artículo 27 Tramitación administrativa automatizada. 3:** Se sugiere añadir al punto la referencia al derecho a no ser objeto de decisiones individuales automatizadas incluida la elaboración de perfiles conforme al artículo 22 del RGPD. Se sugiere la siguiente reacción:

“En caso de tratarse de una actuación administrativa automatizada haciendo uso de sistemas de inteligencia artificial, se adoptarán de forma adicional y específica, cuantas medidas, requisitos y obligaciones resulten necesarias para garantizar la legislación y la ética digital aplicable, atendiendo a un criterio de máximo respeto a los derechos de los interesados, *en particular el derecho a no ser objeto de decisiones automatizadas*.

Se tendrán en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente, promoviéndose la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio.”

EL PRESIDENTE DEL CONSEJO DE TRANSPARENCIA
Y PROTECCIÓN DE DATOS
Jesús María González García

**Dirección General de Estrategia Digital
CONSEJERÍA DE DIGITALIZACIÓN**