4.
Protección de datos y seguridad de la información

El rol del delegado de protección de datos en el sector público y el uso de la IA

Carmen Patricia Mendoza Balladares
Abogada ejerciente, delegada de protección de datos
y docente en Máster Universitario en Derecho Digital UNIR
Universidad Internacional de la Rioja, UNIR
carmenpatricia.mendoza@unir.net

RESUMEN: En el presente artículo, revisaremos como objetivo central el papel que desempeña el Delegado de Protección de Datos (en adelante, DPD), también denominado DPO (Data Protection Officer en inglés) desde sus orígenes y cuáles son sus obligaciones en base a la normativa aplicable, dentro del sector público. A continuación, será palpable la evolución de esta figura, en el contexto específico de la implementación, así como en el uso de la Inteligencia Artificial, analizaremos sus orígenes y concepto, así como los desafíos legales que surgen y la manera en que el DPD puede influir en la implementación ética y responsable teniendo en cuenta el ciclo de vida de los sistemas de IA, garantizando la protección de acuerdo al ciclo de vida de los datos, así como el respeto a los derechos individuales de los ciudadanos en el marco del uso de la Inteligencia Artificial por parte de la Administración Pública.

Palabras clave: Delegado de protección de datos, funciones del DPD, protección de datos, inteligencia artificial, sector público.

ABSTRACT: In this article, we will review the role of the Data Protection Officer (DPO), including its origins and the obligations under the GDPR, within the Public Sector. Next, in the specific context of the integration and use of Artificial Intelligence, we will analyze its history, the legal challenges that arise, and how the DPO can influence the ethical and responsible implementation of these systems. This includes ensuring data protection throughout the lifecycle of AI systems and respecting the individual rights of citizens within the framework of Artificial Intelligence use by Public Administration.

Keywords: Data Protection officer, duties of the DPO, data protection, artificial intelligence (AI), Public Sector

1. CUESTIONES PREVIAS

La figura del delegado de protección de datos está tomando fuerza los últimos años, esto se debió gracias a la llegada de nuevos parámetros, tanto por parte del Reglamento Europeo de Protección de Datos (en adelante, RGPD), así como con la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD). En tal sentido, vamos a estudiar cómo nace esta figura y en cada apartado podemos revisar como va evolucionando y desarrollando sus obligaciones, al igual que lo hacen las tecnologías cada vez más disruptivas y operantes como lo es la Inteligencia Artificial, que plantea nuevas obligaciones para los DPD, aunque para otros sectores todavía viene asentándose y generando mucha incertidumbre y/o preocupaciones.

Entre tales consideraciones, nos vemos viviendo ya en pleno apogeo de la era de la Inteligencia Artificial (en adelante, IA), somos testigos en primera línea sobre la actuación de cada modelo y de los sistemas de esta nueva tecnología, así como su incidencia en la sociedad y en cada uno de los ámbitos; desde la industria, comercio, salud, educación, medio ambiente, hasta la investigación y servicios públicos. Como era de esperar en la Administración Pública vemos como allana el terreno para crear mejoras y agilizar sus procesos.

Entre todo este horizonte disruptivo se asienta el Reglamento IA (en adelante, RIA) que aparece para dar luz a las preocupaciones sobre ética, posibles sesgos que pueden amenazar los derechos fundamentales de los ciudadanos. Esta nueva normativa también denominada AI Act, contiene normas específicas y relativas a los tratamientos de datos que han sido restringidos, como los datos biométricos, así como para las evaluaciones de riesgos. Así mismo esta norma, subraya la importancia de transparencia, brindando nuevas tareas, en modo de nuevas obligaciones a quienes nos encargamos de custodiar los sistemas de gestión de privacidad o las arquitecturas tecnológicas de cumplimiento normativo en materia de protección de datos.

1.1. Orígenes del delegado de protección de datos

Como punto de partida, para poder analizar esta figura, nos remontamos a la década de los setenta en Alemania, concretamente la figura aparece en el año 1977 con la *"Bundesdatenschutzgesetz"* o Ley Federal de Protección de Datos de Alemania, cuyo artículo 28 versa sobre el nombramiento de un delegado de protección de datos (Rodríguez Ayuso, 2021). Es así que, desde entonces, se observaba ya la necesidad e importancia de que exista una persona que sepa orientar sobre cómo se llevará a cabo el tratamiento de datos.

A continuación, el artículo 29 del mismo cuerpo legislativo, describe las tareas o funciones del delegado de protección de datos. Responsabilidades que reflejaban una perspectiva adelantada para su tiempo. Visto desde una panorámica actual, estas funciones se centraban en un aspecto general, teniendo una visión global de los tratamientos de los datos para poder llevar un buen control, pero también, se centraba ya en aspectos más críticos en el marco de los tratamientos de datos personales, como es la formación a los trabajadores y los procesos de selección;

> «*…mantener una visión general del tipo de datos personales almacenados y de los fines y objetivos comerciales para los cuales se requiere el conocimiento de estos datos, controlar el uso adecuado de los programas de procesamiento de datos, familiarizar a las personas involucradas en el procesamiento de datos personales con las disposiciones legales pertinentes y brindar asesoramiento en la selección de personal para el tratamiento de datos personales*».

Posteriormente, es en la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. En el considerando 49, de dicha Directiva podemos apreciar, también una alusión a la figura de *"persona encargada de protección de datos" a la que se le dota de independencia"*; *"… que la persona encargada de la protección de los datos, sea o no empleado del responsable del tratamiento de datos, deberá ejercer sus funciones con total independencia"*. En la Directiva 95/46/CE, no se menciona o se obliga la designación o nombramiento de un delegado de protección de datos, tampoco se describe la figura por lo que en España tampoco se instaura de forma oficial. No obstante, varios países contemplaron la figura del *Data Protection Officer*, como, Países Bajos, Francia o Luxemburgo (Rodríguez Ayuso, 2021).

Finalmente, es el Reglamento General de Protección de Datos (en adelante, RGPD) publicado y en vigor en 2016, aplicable desde mayo de 2018, que introdujo grandes y notables cambios, posicionando a los delegados de protección de datos como parte esencial para las organizaciones, proporcionando un apoyo fundamental para el cumplimiento del RGPD. Sin embargo, es extraño de ver múltiples definiciones en el artículo 4. RGPD y no encontrar entre ellas una definición del delegado de protección de datos. Si queremos estudiar a fondo

la nueva figura, tenemos que acudir a la sección 4 artículos 37; designación, 38; posición y funciones contenidas en el artículo 39 del RGPD.

Siendo obligatoria la designación de un DPD cuando el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial. (Art. 37.1 RGPD) Adicionalmente continúa el texto indicando que se podrá designar un único DPD para varias autoridades u organismos públicos, en atención a su tamaño y estructura organizativa. (Art. 37.3 RGPD). En este sentido desde la AEPD, se concretó la fecha límite para la designación de los DPD en el ámbito público, que debía de hacerse antes de la fecha prevista para que fuera de aplicación, el 25 de mayo de 2018. Habiendo pasado ya más de 5 años podemos observar que el delegado de protección de datos es una figura que ya tiene cierto bagaje en el sector público, por lo que de forma paulatina en múltiples casos ya está tomando parte en la implementación de nuevas tecnologías, así como el uso de la Inteligencia artificial.

Por otra parte, la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en adelante, LOPDGDD) vino a complementar y desarrollar el RGPD (Capítulo III, artículos 34 al 37 RGPD). Vemos como el artículo 34. parte de los supuestos previstos para la designación obligatoria especificando un poco más los sujetos obligados. El artículo 35, nos habla sobre la cualificación y que se centra en tener conocimientos especializados, bien a través de certificación, que tendrán en cuenta la obtención de una titulación universitaria y la práctica en este ámbito. Por su parte el artículo 36 versa sobre cuál es su posición respecto de las organizaciones, su independencia y funciones inspectoras para garantizar que no se vulnere el derecho fundamental a la protección de datos. Así mismo, como debe ser su relación entre la autoridad de control y otras entidades que actúen como encargados del tratamiento. Que se detalla con mayor claridad ante casos de reclamaciones por parte de afectados ante la autoridad de control, AEPD y cómo debe desarrollar su intervención como lo estipula el artículo 37. Como apreciamos ambas normativas; RGPD y LOPDGDD, han tenido un impacto directo en el sector público en lo relativo a la función del delegado de protección de datos cuyo encuadre está también muy ligado a la publicidad activa y el acceso a la información pública. Así como las obligaciones establecidas por la legislación autonómica (Mendoza Balladares, 2024).

1.2. Identificación de roles en el ámbito público

Visto lo anterior, comenzaremos por comprender los roles involucrados, ya que en el ámbito de la protección de datos y la Administración General del Estado (en adelante, AGE), así como de la Administración Autonómica y Local debe dejarse claro que nos encontramos con aplicación de otra normativa sectorial porque muchos de los tratamientos de datos son servicios públicos. Como ejemplos tenemos; la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley 39/2015, de 1 de octubre, del

Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. Todas ellas muy presentes en los diversos tratamientos de datos personales.

a) Identificación del responsable del tratamiento de datos en el sector público.

El RGPD, nos dice que puede ser una autoridad pública[1] o cualquier otro organismo, además de una persona física o jurídica, y viene a ser aquel que determina los fines y medios del tratamiento. En el contexto de la Administración General del Estado, podemos tomar de ejemplo un responsable del tratamiento de los datos, que sería; la Secretaría General de Coordinación Territorial, de la Subdirección General de Recursos Humanos de la Administración General del Estado en el Territorio o por variar un poco más como otro responsable; la Delegación del Gobierno contra la Violencia de Género. Igualmente, en el contexto de la Administración Autonómica, tendríamos al Gobierno de Canarias, y en el ámbito Local, esta responsabilidad recae en los municipios, diputaciones provinciales e islas, según la normativa local. En este sentido, cualquier Ayuntamiento es un responsable del tratamiento de datos, como, por ejemplo, el Ayuntamiento de Santa Cruz de Tenerife.

Adicionalmente, las diputaciones provinciales, consejos y cabildos insulares gestionan sus propios tratamientos de datos. Podemos poner de ejemplo como responsable de tratamiento de datos, al Cabildo Insular de la Palma. Además, entidades de ámbito territorial inferior al municipal, como comarcas y áreas metropolitanas, también pueden ser responsables del tratamiento. Esta responsabilidad se extiende a entidades como organismos autónomos y entidades públicas empresariales locales (AEPD, 2023). Considerando la extensa y diversa gama de entidades y organizaciones a las que se aplica esta normativa, la función del DPD dentro de estas instituciones y entidades deberá ajustarse a las características particulares de cada una de ellas. (Saíz Peña y Balanzategui Vidal, 2019)

b) Identificación de los encargados de tratamiento en el sector público

Dado que el responsable del tratamiento es quién debe evaluar que los encargados del tratamiento ofrezcan garantías de cumplimiento del RGPD antes de contratar sus servicios. Afirmamos entonces vía RGPD, que serán encargados del tratamiento cualquier persona física, jurídica, autoridad pública, servicio u otro organismo, que trate datos por cuenta del responsable (que en nuestro caso es una autoridad pública). Además, es necesario revisar y adecuar los contratos

---

[1] RGPD, ni LOPDGDD, especifican quienes pueden formar parte de una "Autoridad Pública". Según interpretación del criterio del GT29, serían Administraciones Públicas; estatales, autonómicas y locales, organismos públicos dependientes de las AAPP. Otras instituciones con funciones similares a las administrativas. Entidades privadas que realizan actividades de interés público, ya sean dependientes de autoridades públicas o no y personas físicas o jurídicas privadas que realizan funciones de interés público, como empresas con contratos de concesión.

de encargo de tratamiento a las previsiones del RGPD, que incluye un contenido mínimo (Art.33.5 LOPDGDD y art. 28 RGPD). El artículo 33.5 de la LOPDGDD indica que, en el sector público, las competencias propias de un encargado del tratamiento pueden asignarse a un órgano específico de la Administración o a organismos autónomos vinculados o dependientes. Esta asignación debe realizarse a través de una norma que regule sus competencias e incorpore el contenido exigido por el artículo 28.3 del RGPD.

Por su parte, la Ley 9/2017, de 8 de noviembre, de contratos del sector público (LCSP), prevé en su disposición adicional 25ª que cuando la contratación implique el acceso del contratista a datos personales de cuyo tratamiento sea responsable la entidad contratante, el contratista tendrá la consideración de encargado del tratamiento. En estos casos también será de aplicación el RGPD.

c) Identificación de los destinatarios

Se denomina destinatario a aquella persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, distinguiendo que puede ser un tercero o no. El RGPD, advierte además que, no se considera destinatario a aquellas autoridades públicas que en el marco de una investigación concreta traten con datos personales; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a cada finalidad u objetivo del tratamiento.

Podrán ser destinatarios por ejemplo dentro de un Ayuntamiento, otras Administraciones públicas, el Defensor del Pueblo, Juzgados y Tribunales de Justicia, Fuerzas y Cuerpos de Seguridad, siempre en función al tratamiento de datos específico.

d) Identificación del Tercero

Viene a ser la persona física o jurídica, autoridad pública, servicio u organismo que será diferente del sujeto interesado o titular de los datos, del responsable del tratamiento, del encargado del tratamiento y personas autorizadas a tratar datos bajo las instrucciones del encargado o responsable. Esto quiere decir que participa en el tratamiento de datos y no sólo se le comunican los datos personales.

Identificar esta figura puede ser muy importante en el ámbito de las nuevas tecnologías, recordemos que existen muchos otros roles en la puesta en marcha de un sistema de Inteligencia Artificial como veremos más adelante.

e) Autoridades autonómicas de protección de datos

Además de la autoridad de control que es la Agencia Española de Protección de Datos, según lo establecido en los art. 57 y 58 RGPD, donde se indican sus funciones y poderes. El art. 57 de la LOPDGDD, señala que tendrán las mismas funciones y poderes las autoridades autonómicas de protección de datos, podemos citar a la Autoridad Catalana de Protección de Datos, el Consejo de Trans-

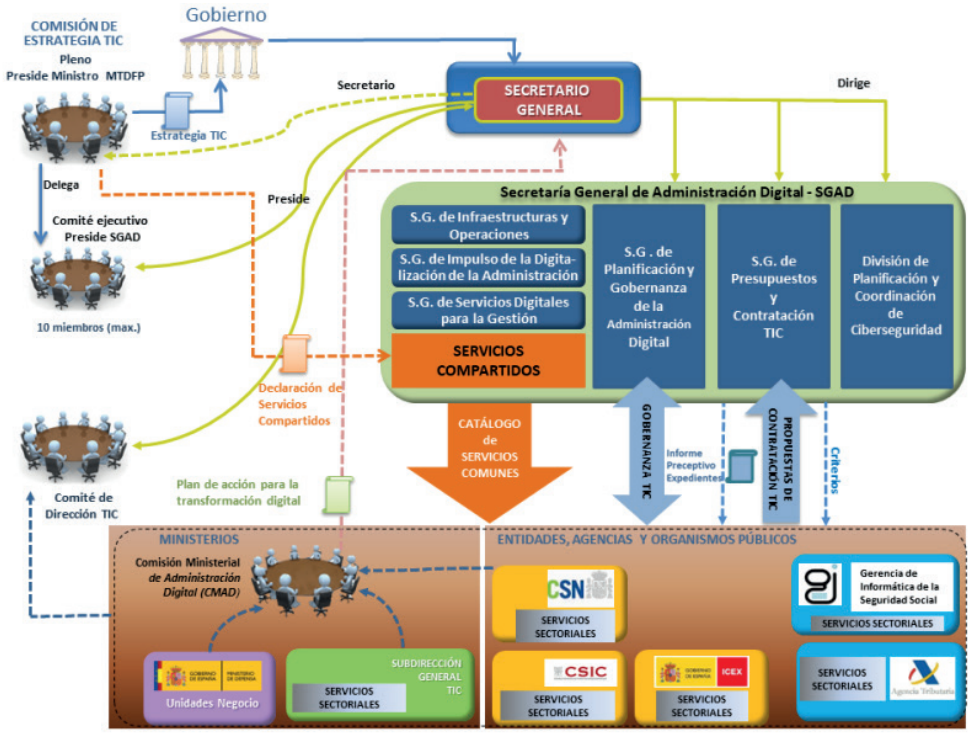
parencia y Protección de Datos de Andalucía y la Agencia Vasca de Protección de Datos. Limitando sus competencias a tratamientos de datos en el sector público de la Comunidad Autónoma, funciones públicas locales y tratamientos previstos en los Estatutos de Autonomía. Además, estas autoridades pueden emitir circulares similares a las de la Agencia Española de Protección de Datos para los tratamientos de su competencia. Cuando la autoridad competente sea una autoridad autonómica de protección de datos, se estará a su normativa de aplicación en lo que ha sanciones se refiere. Art.76 LOPDGDD. Esto además nos indica que, si una persona no decide acudir directamente a la AEPD, puede remitir su reclamación ante el DPD de cualquier organismo público, quién deberá de adoptar una decisión el en plazo de 2 meses. Sobre la comunicación de datos de los administrados a cualquier sujeto que solicite los mismos, nos dice que debe mediar el consentimiento o puede ampararse en un interés legítimo si prevalece sobre los derechos e intereses de los administrados.

f) Estrategia TIC en la Administración General de Estado (AGE)

En clave muy diversa, resulta interesante mencionar la Estrategia TIC, de la Administración General del Estado que establece el marco global para la transformación digital de la Administración. Definiendo principios, objetivos, acciones para el desarrollo progresivo de la Administración Digital. No podemos pasar por alto la presencia del DPD en cualquier estrategia de transformación digital, puesto que debe garantizar que todas las acciones y servicios compartidos cumplan con las normativas de protección de datos. Como órgano máximo de gobernanza tenemos a la Comisión de Estrategia TIC que incluye representantes de todos los Ministerios y actúa como vínculo entre los objetivos gubernamentales y el uso de las TIC en la Administración. Sus funciones principales engloban elaborar y proponer la Estrategia TIC al Consejo de ministros, declarar medios y servicios compartidos, priorizar proyectos. Además, informará anualmente al Consejo de ministros sobre el estado de la transformación digital. Podemos apreciar en la figura número 1, cual es el modelo de Gobernanza TIC, dentro de la Administración General del Estado, para situarnos en el contexto de la AGE. Ya que más adelante abordaremos la Estrategia Nacional de Inteligencia Artificial, (en adelante, ENIA) en la que viene trabajando el Gobierno de España.

En términos fácticos, tras ver el Informe de la década digital,2023, resulta evidente que ahora mismo España tiene muy buenos indicadores que le están posicionando por encima del promedio de la Unión Europea. Reflejando así el compromiso en las estrategias y planes que viene implementando. Con un 84 % de ciudadanos que utilizan servicios de la Administración electrónica, frente a la media que es un 74%, siendo Dinamarca el país que lleva la delantera con un 98.9 %. España además se perfila como un país con mejor desempeño en infraestructura digital un 93%, en particular en conectividad. En redes fijas de muy alta capacidad está significativamente por encima de la media de la UE, que es un 73%.

Figura 1. Modelo de Gobernanza TIC



Fuente: Administración Electrónica.gob.es[2]. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Organizacion/ambito-AGE.html

2. EL ROL DEL DELEGADO DE PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN PÚBLICA

2.1. Posición del DPD en el sector público

Una de las primeras cuestiones a dilucidar es justamente saber qué lugar ocupa un DPD en las organizaciones administrativas y nos dice la AEPD, que debido a las responsabilidades que conlleva su cargo, debe estar ubicado dentro de órganos o unidades que posean competencias y funciones que abarquen varios departamentos o áreas de la organización. Además, el nivel del puesto de trabajo

[2] Si se quiere ampliar información y revisar los diversos Planes de Transformación digital se puede ampliar la información en. https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Plan_Digitalizacion_AAPP/planes-anteriores.html

del DPD debe ser apropiado para facilitar la comunicación y la interacción con la dirección del órgano u organismo donde desarrolla sus funciones. Garantizando en todo momento su independencia.

En todo caso el DPD, puede estar respaldado formalmente por una unidad específica dedicada a la protección de datos, especialmente en estructuras más grandes, como lo es un Ministerio por ejemplo. Sin embargo, en estructuras más pequeñas, el DPD puede tener que combinar sus funciones con otras responsabilidades. En tales casos, es fundamental evitar conflictos de intereses respecto de otros deberes y tareas. El rol del DPD implica actuar como asesor y supervisor interno, por lo que no debe ocuparse por personas que también estén encargadas de tomar decisiones sobre tratamientos de datos o sobre cómo se manejarán los datos, como puede ser el responsable de seguridad, por ejemplo.

La posición del DPD, implicaría entonces según el RGPD, a) no recibir instrucciones sobre cómo desempeñar sus funciones y no ser destituido ni sancionado por el responsable o encargado debido a su desempeño. b) tener una participación adecuada y oportuna en todas las cuestiones relacionadas con la protección de datos personales. c) recibir apoyo del responsable o encargado, quienes deben proporcionarle los recursos necesarios para el desempeño de sus funciones y d) rendir cuentas directamente al más alto nivel jerárquico del responsable o encargado. Esto significa que debe poder interactuar con niveles jerárquicos capaces de tomar o promover decisiones basadas en sus recomendaciones, propuestas o evaluaciones.

Respecto de su independencia, los DPD no tienen autoridad para tomar decisiones más allá de sus responsabilidades definidas en el Artículo 39. La responsabilidad de cumplir con las leyes de protección de datos recae en el responsable del tratamiento de datos, quien debe poder demostrar dicho cumplimiento. Si el responsable del tratamiento toma decisiones que contradicen el RGPD y el consejo del DPD, este último debe tener la oportunidad de expresar su oposición. (GT29, 2017) De igual forma queda claro que un delegado de protección de datos no puede ejercer funciones para determinar los fines y los medios del tratamiento de datos personales del responsable del tratamiento o de su encargado.[3] También nos adelanta AEPD que puede surgir conflicto de intereses, por ejemplo, si se pide a un DPD que represente al responsable o al encargado del tratamiento ante los tribunales en casos sobre protección de datos. (Gabinete jurídico 0038/2023 AEPD).

A) Procedimiento de adjudicación en la Contratación de DPD

En este marco, cuando no haya una designación interna del DPD dentro de la autoridad pública, se establece un complejo régimen jurídico del contrato y

[3] Sentencia del Tribunal de Justicia de la Unión Europea de 9 de febrero de 2023, asunto C-453/21 Caso X-FAB Dresden GmbH & Co. KG contra FC.

un procedimiento de adjudicación específico para garantizar la transparencia, eficacia y legalidad en la selección de los DPD. Mediante la cual, se aplicará preferentemente las cláusulas y Anexos, contenidos en los pliegos de contratación o también pliego de prescripciones técnicas, que revisten carácter contractual. La adjudicación se llevará a cabo a través de un proceso abierto simplificado, específicamente en su modalidad abreviada, (Art. 159.6 LCSP) [4]

En todo lo que puedan contravenir las normas serán de aplicación; la Ley Reguladora de las Bases de Régimen Local (en adelante, LBRL) y consecuentemente, la LCSP, el Real Decreto 817/2009, de 8 de mayo, que desarrolla parcialmente la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público. El Real Decreto 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento General de la Ley de Contratos de las Administraciones Públicas (en adelante, RCAP), en su nueva redacción vía el RD 773/2015, de 28 de agosto. Así como, restantes preceptos de la LCSP, del Real Decreto 817/2009 y del RCAP. Supletoriamente se regirán por las demás normas de Derecho Administrativo; la Ley 39/2015, del Procedimiento Administrativo Común y normas complementarias. En defecto de todo lo anterior, se aplicarán las normas de Derecho Privado.

B) Posibilidad de apercibimiento en el sector público

Cuando cualquier organismo u órgano público, esté inmerso en un procedimiento sancionador, será posible que la resolución conlleve como sanción un apercibimiento que incluirá medidas correctoras. Dicha resolución seguirá el mismo curso que las demás, publicándose en la página web de la AEPD, pero en este caso se identificará al infractor, órgano responsable de la infracción, hasta el superior jerárquico, notificándose también al Defensor de Pueblo y publicándose en el Diario Oficial que corresponda. La resolución no termina con el pago de una cantidad a efectos económicos, pues es un mero apercibimiento o amonestación, pero puede proponer un procedimiento disciplinario.

2.2. Funciones del delegado de protección de datos

Las funciones del delegado de protección de datos (en adelante, DPD) en las administraciones públicas son similares a las de cualquier otra organización, pero tienen sus propias características debido a cada propio esquema organizacional y por tanto cada tratamiento de datos. Tengamos en cuenta que la mayoría de administraciones presta servicios públicos por los que debe de recabar información personal de los ciudadanos. En la Guía práctica sobre las funciones del DPD, del Manual del DPD detalla un esquema muy interesante y que siempre solemos

[4] Ley 9/2017, de 8 de noviembre por el que se aprueba la Ley de Contratos del Sector Público (en adelante, LCSP) que utiliza criterios cuantificables que se evaluarán exclusivamente mediante la aplicación de fórmulas para la adjudicación. Además, vía art.347 LCSP, se pone a disposición, el perfil de contratante en la Plataforma de Contratación del Sector Público.

comentar con los estudiantes en clase. Las funciones indicadas en el RGPD están muy bien y resumidas, pero el delegado de protección de datos, no sólo debe ceñirse a la lista del artículo 39 que vemos en la mayoría de textos académicos, hacerlo sería limitarse mucho el trabajo. Con el conocimiento amplio de la normativa, estas funciones se extienden desde el estudio de la situación inicial de la organización, que nos permita conocer ese punto de partida para empezar, hasta el informe anual, pautado en su calendario para que pueda ir desempeñando sus funciones genéricas de asesorar, informar, supervisar, entre otras.

2.2.1. Función sobre el conocimiento del contexto o situación inicial

En el ámbito de las administraciones públicas, la función preliminar del DPD, implica definir el alcance del entorno del responsable y elaborar un mapa de las actividades de tratamiento de datos de la organización. En términos generales, solemos denominar un mapeo de datos por tratamientos de datos, que consiste en identificar todas y cada una de las operaciones de tratamiento de datos. Para llegar a esto, primero se requiere un conocimiento completo de la distribución interna, conociendo el organigrama y también la asignación de roles y las responsabilidades relacionadas con el tratamiento de datos, así como los enlaces y acuerdos externos con otras organizaciones y el marco legal aplicable.

Como ejemplo ilustrativo podemos ver la estructura organizativa del registro de tratamientos del Gobierno de Canarias, que lo componen, la Presidencia y 12 Consejerías:

Figura 2. Estructura organizativa Gobierno de Canarias

1. Presidencia del Gobierno, que además se divide en:
   - Viceconsejería de la Presidencia
   - Dirección General de Transformación Digital de los Servicios Públicos.
   - Viceconsejería de Acción Exterior
   - Dirección General de Emigración
   - Viceconsejería de Comunicación y Relaciones con los Medios
   - Dirección General de Comunicación
   - Secretaría General
   - Consejo Económico y Social
   - Dirección General del Gabinete de la Vicepresidencia próxima a extinguirse.
   - Dirección General de Investigación y Coordinación del Desarrollo Sostenible próxima a extinguirse.
   - Dirección General del Gabinete del presidente, próxima a extinguirse.
2. Consejería de Sanidad
3. Consejería de Economía, Industria, Comercio y Autónomos.
4. Consejería de Hacienda y Relaciones con la Unión Europea.

5. Consejería de Presidencia, Administraciones Públicas, Justicia y Seguridad.
6. Consejería de Educación, Formación Profesional, Actividad Física y Deportes
7. Consejería de Política Territorial, Cohesión Territorial y Aguas
8. Consejería de Turismo y Empleo
9. Consejería de Universidades, Ciencia e Innovación y Cultura
10. Consejería de Transición Ecológica y Energía
11. Consejería de Bienestar Social, Igualdad, Juventud, Infancia y Familias
12. Consejería de Agricultura, Ganadería, Pesca y Soberanía Alimentaria
13. Consejería de Obras Públicas, Vivienda y Movilidad

Información recogida de la web del Gobierno de Canarias

Asimismo, cada Consejería también la conforma una propia estructura interna con una Secretaría General, Viceconsejería, varias direcciones generales y otros órganos o unidades. Para poder continuar ilustrando el ejemplo a modo directo, podemos observar que, dentro de la Consejería de Hacienda y Relaciones con la Unión Europea, tenemos, la Secretaría General Técnica, las direcciones generales de Planificación y Presupuesto, Patrimonio y Contratación, Asuntos Europeos, el Instituto Canario de Estadística, la Agencia Tributaria Canaria, el Tribunal Administrativo de Contratos Públicos y la Intervención General. Como ya se puede intuir el organigrama del Gobierno de Canarias es amplio y quizás requerirá un equipo de trabajo encabezado por un delegado de protección de datos, que se encargue de ejecutar el resto de funciones que vamos a desarrollar o en función al organigrama, pueden designarse diversos DPD por cada Consejería u órganos independientes.

Otra cuestión previa es identificar normativa aplicable para cada tratamiento, pues está claro que partimos como base del RGPD y LOPDGDD en materia de protección de datos. Las administraciones públicas además deben de cumplir con otra legislación autonómica o nacional, como por ejemplo el Esquema de Seguridad Nacional (en adelante, ENS) en lo relativo a medidas de seguridad aplicables, lo veremos al estudiar uno de los tratamientos, el voto accesible de la figura nº 3 y 4.

2.2.2. Funciones de tipo organizativo

Dentro de estas funciones el Manual del DPD, nos sitúa, en al menos otras cuatro que son; la creación de un registro de operaciones de tratamiento de datos personales, su revisión continua, realizar un análisis de riesgos, y gestionar aquellos cuyo resultado se hubiera obtenido un alto riesgo, para entonces realizar una Evaluación de Impacto de Protección de datos o EIPD.

Respecto a la creación del registro de actividades del tratamiento, se debe de realizar el mapeo de datos partiendo del organigrama, para poder identificar los

tratamientos y si son conformes a los principios de la protección de datos, como ejemplo podemos observar el tratamiento *de Voto accesible,* que lo identificamos dentro de la Dirección General de Transparencia y participación ciudadana de la Consejería de Presidencia, Administraciones Públicas, Justicia y Seguridad. Cada órgano administrativo deberá identificar los tratamientos de datos para darle forma al RAT, podemos ya observar que es un documento bastante amplio. Encontramos la lista de los tratamientos que se encuentran cada uno definidos conforme las exigencias del art. 30 RGPD y del art. 31.1 LOPDGDD. Además, tal y como indica el art.31.2 los sujetos del art. 77.1, que tendrán la obligación de hacer público el Registro de Actividades del tratamiento (en adelante RAT), que debe ser además accesible en el entorno virtual, constando además la base legal, que desde ahora indicamos que deberá cumplirse con el deber de información tal y como lo indica los arts. 13 y 14 del RGPD.

Los sujetos a los que aplica como en nuestro caso estaría contemplado en el apartado c del art. 77.1, c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

Figura 3. Tratamiento de datos, voto accesible y finalidades.

Órgano Administrativo	Tratamientos de datos
Dirección General de Transparencia y Participación Ciudadana de la Consejería de Presidencia, Administraciones Públicas, Justicia y Seguridad.	***Voto Accesible:*** ***Finalidades:*** • Gestión del procedimiento para el voto accesible (*Kit Voto Accesible*). • Gestión de pagos por participación en los procesos electorales al Parlamento de Canarias. • Formulario de contacto del Portal de Datos Abiertos de Canarias. • Publicidad Activa. • Participación ciudadana. • Gestión de la base de datos de representantes de la administración en los procesos electorales al Parlamento de Canarias. • Ejercicio de derechos en materia de protección de datos. • Acceso a la información pública. • Publicación de conjuntos de datos en el Portal de Datos Abiertos de Canarias. • Registro de Parejas de Hecho de la Comunidad Autónoma de Canarias. • Registro de Asociaciones de la Comunidad Autónoma de Canarias.

Órgano Administrativo	Tratamientos de datos
	• Registro de Fundaciones de la Comunidad Autónoma de Canarias. • Protectorado de Fundaciones de Canarias. • Registro de Colegios Profesionales de la Comunidad Autónoma de Canarias.

Elaboración propia, basada en el Registro de Actividades del Tratamiento de Datos (RAT) del Gobierno de Canarias.

Si elegimos el tratamiento de ***Voto accesible***, de la Figura nº 3, por ejemplo, el delegado de protección de datos deberá de partir del marco normativo aplicable, para poder continuar con su elaboración tomando en cuenta que pueden existir excepciones o más obligaciones, según el tratamiento. Al respecto, tenemos por ejemplo que acudir al Real Decreto 1612/2007 de 7 de diciembre, por el que se regula el procedimiento de voto accesible que facilita a las personas con discapacidad visual el ejercicio del derecho de sufragio. Posteriormente también podemos tener en cuenta el Decreto 99/2011, de 27 de abril, por el que se regulan las condiciones de locales, urnas, papeletas y sobres y demás elementos materiales a utilizar en las elecciones al Parlamento de Canarias. En la figura nº 4, vemos como ampliamos ese Registro de Actividades del Tratamiento, sobre el tratamiento *Voto accesible* y sólo sobre la finalidad; gestión del procedimiento para el voto accesible. Lo que ya nos debe quedar claro que el Registro de Actividades del Tratamiento es un Documento que no puede tomarse a la ligera pues debemos de desarrollarlo en función a cada tratamiento de datos y finalidades de forma individual. Podemos observar, además, que se tratan datos especialmente protegidos y el DPD, deberá de constantemente revisar que se apliquen las medidas de este tratamiento, debido a que es obligatorio que se realice además una adecuada gestión del riesgo o si procede una Evaluación de Impacto de Protección de Datos, si se encontrase un alto riesgo de estas operaciones del tratamiento de datos.

Figura 4. Desarrollo del RAT, para el tratamiento: Voto accesible.

REGISTRO DE ACTIVIDADES DEL TRATAMIENTO	
RESPONSABLE	Dirección General de Transparencia y Participación Ciudadana. **(Aquí se añaden los datos de contacto)**
TRATAMIENTO	Voto Accesible[5],

[5] Podemos ampliar el procedimiento para el voto accesible para personas ciegas con discapacidad visual en: https://infoelectoral.interior.gob.es/es/proceso-electoral/visitas-virtuales/el-voto-accesible/index.html

REGISTRO DE ACTIVIDADES DEL TRATAMIENTO	
BASE LEGITIMADORA	El tratamiento resulta necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (art. 8 LOPDGDD). Real Decreto 1612/2007de 7 de diciembre, por el que se regula en procedimiento de voto accesible que facilita a las personas con discapacidad visual el ejercicio del derecho de sufragio.
FINALIDADES	Gestión del procedimiento para el voto accesible. *(kit voto accesible)*
CATEGORÍA DE PERSONAS INTERESADAS. (Viene preestablecido en la normativa de aplicación)	Personas físicas con discapacidad visual que conozcan el sistema de lecto-escritura Braille y tengan reconocido un grado de minusvalía igual o superior al 33 por 100 o sean afiliados a la Organización Nacional de Ciegos Españoles, que deseen utilizar el procedimiento de voto accesible regulado en el Real Decreto 1612/2007, de 7 de diciembre.
CATEGORIAS DE DATOS PERSONALES	**Datos de carácter identificativo:** DNI/NIF/documento identificativo, nombre y apellidos, dirección y teléfono. **Datos especialmente protegidos:** (Datos de salud) Grado de discapacidad visual igual o superior al 33% y afiliación a la ONCE.
CESIÓN DE DATOS	Instituto Nacional de Estadística (Oficina del Censo Electoral), entidades Locales, autoridades judiciales y otras administraciones públicas cuando la cesión esté prevista por ley.
TRANSFERENCIAS INTERNACIONALES DE DATOS	No se contemplan
TIEMPO DE CONSERVACIÓN DE LOS DATOS	Durante el tiempo necesario para cumplir con la finalidad para determinar posibles responsabilidades. Antes de su eliminación se realizará un estudio de valoración documental para analizar el posible valor informativo, de investigación o histórico. A tal fin, le será de aplicación lo dispuesto en la normativa de gestión documental y archivos de la Administración Pública de la Comunidad Autónoma de Canarias y, en su caso, en la normativa sectorial.
MEDIDAS DE SEGURIDAD	Aplicables las medidas de seguridad previstas en el Capítulo IV del Título VIII del Real Decreto 1720/2007, de 21 de diciembre, respecto del tratamiento no automatizado de los datos, en tanto no se oponga o resulte incompatible con el Reglamento (UE) 2016/679 Son aplicables las medidas de seguridad del Anexo II (Medidas de seguridad) del Real Decreto 311/2022, de 4 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Elaboración propia. Basada en información contenida en el RAT del Gobierno de Canarias.

Visto lo anterior, podemos darnos cuenta que con sólo empezar a identificar los tratamientos de datos, ya se inicia la función de revisión constante y en conformidad con el RGPD, pues debemos de identificar la base legitimadora, para todas y cada una de las finalidades. En función de las mismas, nos encontramos que puede ser aplicable alguna normativa local tal y como venimos mencionando. En adelante, valoraremos las categorías de datos, tipos de datos, si hay cesión de datos o no, transferencias internaciones de datos, el tiempo de conservación e identificar las medidas de seguridad. Según vemos en la Figura nº3 y en cumplimiento de los Arts. 5, 6, 13, 14, 30 RGPD, así como el Art. 31 de la LOPDGDD en lo relativo a su publicación online. Quizás lo que más preocupe a un DPD en el marco de sus obligaciones es poder desarrollar una buena identificación o mapeo de datos para plasmarlo y estructurarlo en la Política de Protección de Datos, ya que posteriormente debe de embarcarse en otra función de mayor complejidad que es iniciar una correcta gestión de riesgos para luego desarrollar una Evaluación de Impacto en Protección de datos o EIPD. Estamos viendo que en el marco de las funciones de tipo organizativo tiene cabida el asesoramiento, así como brindar la debida información tanto al responsable del tratamiento como a los encargados. En este sentido en lo relativo al RAT, debe de elaborarse también respecto de los encargados del tratamiento.

Dentro del ámbito de las Administraciones Públicas, deben de verificarse los riesgos asociados a los tratamientos de datos, existiendo técnicas de análisis de riesgos que se centran principalmente en la seguridad de la información que se ampliarán y complementarán para incluir riesgos asociados a la protección de datos. Desde esta perspectiva, la Agencia Española de Protección de Datos, está colaborando estrechamente con el Centro Criptológico Nacional. Ya que la aplicación de las medidas de seguridad vemos que toma los criterios establecidos en el ENS. (FEMP, 2017)

En relación a la función de una evaluación de impacto, EIPD, requiere que esta sea con una metodología paso a paso y forma parte de la gestión de los riesgos. Empezaremos por determinar si los tratamientos de datos dentro del ciclo de vida de los datos, requieren una EIPD, debido a su potencial para generar riesgos significativos (alto riesgo) para los derechos y libertades de las personas afectadas, y disponer de ese enfoque metodológico para llevar a cabo esta evaluación. RGPD enumera ciertas situaciones en las que se considerará que existe este alto riesgo y sugiere que las autoridades de control, pueden publicar listas adicionales de procesos de alto riesgo. (Art. 35.4 RGPD)[6] Además, el RGPD especifica los elementos mínimos que deben incluirse en estas Evaluaciones de Impacto en Materia de Protección de Datos:

---

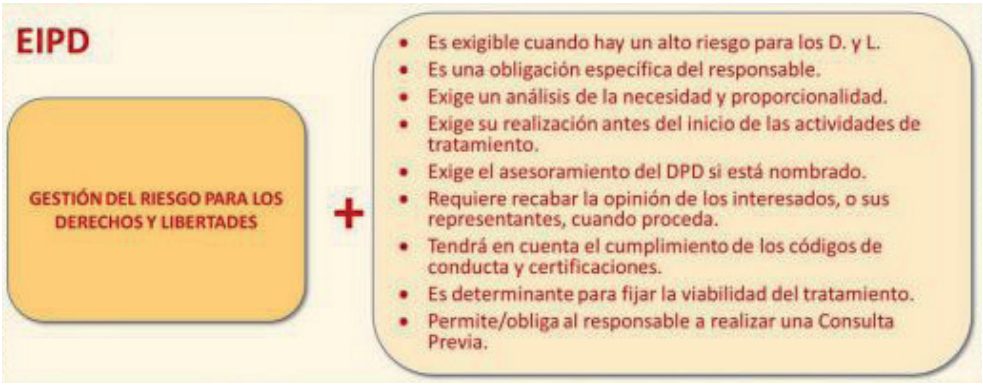
[6] Según el Manual del DPD (Korff y Georges 2019). 22 de las 28 Autoridades de control fueron quienes comunicaron estas listas al CEPD. La AEPD, está entre ellas, fue una de las autoridades de control que publicaron listas de tipos de tratamientos que requieren una Evaluación de impacto en protección de datos. Disponible en: https://www.aepd.es/documento/listas-dpia-es-35-4.pdf

- Descripción del tratamiento de datos: con detalles "sistémicos" sobre los datos personales involucrados, el propósito del tratamiento y los métodos utilizados.
- Evaluación de la necesidad y proporcionalidad: mediante un análisis de si el tratamiento de datos es necesario para alcanzar los objetivos previstos y si es proporcionado en relación con los riesgos para los derechos y libertades de las personas afectadas.
- Evaluación de los riesgos: se realizará una identificación y evaluación de los riesgos para los derechos y libertades de los individuos, incluyendo la posibilidad de discriminación, daño a la reputación, pérdida de control sobre los datos, entre otros.
- Medidas de mitigación: mediante la elaboración de planes de acción a corto, mediano y largo plazo, describiendo las medidas técnicas y organizativas que se implementarán para mitigar los riesgos identificados, incluyendo medidas de seguridad, protección de datos por diseño y por defecto, y políticas de retención de datos.
- Consulta: involucraremos a todas las partes interesadas, los propietarios de los riesgos de cada área, departamento o unidad, además de los responsables del tratamiento, los interesados y las autoridades de protección de datos, en el proceso de evaluación.
- Gestión documental: se llevará un registro detallado de los resultados de la evaluación, mediante informes, incluyendo los riesgos identificados, las medidas de mitigación propuestas y las decisiones tomadas.
- Revisión y seguimiento: se implementarán procesos para revisar y actualizar periódicamente la Evaluación de Impacto en Protección de Datos a medida que cambian las circunstancias del tratamiento de datos o se identifican nuevos riesgos, mediante un cronograma.

No obstante, cuando los tratamientos de datos estén asociados a la consecución de objetivos de interés público o estén relacionados con el ejercicio de poderes públicos, el RGPD contempla la posibilidad de no llevar a cabo una Evaluación de Impacto, incluso si se trata de procesos con alto riesgo. Esto ocurre cuando la normativa sectorial regula el funcionamiento o conjunto de operaciones de tratamiento, y ya se ha realizado una evaluación de impacto sobre la protección de datos como parte de una evaluación general en el contexto de la adopción de dicha normativa de ámbito público, como ocurriría por ejemplo en el plan de adecuación de cualquier Administración Pública al Esquema Nacional de Seguridad.

De igual manera, desde otra perspectiva y en el marco de iniciativas legislativas por parte de las AAPP, nos recalcan que esta EIPD, no sería una evaluación de riesgo legal o de cumplimiento. Debe evaluarse cuál es el impacto real en cada tratamiento de datos respecto de los derechos fundamentales de las personas físicas y como sociedad en conjunto (AEPD, 2023)

Figura 5. EIPD



Fuente: AEPD.

Como vemos, un especialista debe de conocer muy bien todas las cuestiones relativas a la EIPD pues adicionalmente, RGPD y AEPD, (antes de la llegada de RIA) en su lista nos indica que cuando se utilicen nuevas tecnologías, toma de decisiones automatizadas, se considerará siempre que existe alto riesgo, como podrá ser el caso por ejemplo de la Inteligencia Artificial.

Figura 6. Resumen de la evaluación de la necesidad, idoneidad y proporcionalidad de un tratamiento

EVALUACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD	
OBJETIVO DEL TRATAMIENTO: "VOTO ACCESIBLE"	Garantizar que las personas con discapacidad visual puedan ejercer su derecho al voto de manera autónoma y confidencial, conforme a lo estipulado en el Real Decreto 1612/2007, de 7 de diciembre. Este procedimiento es fundamental para asegurar la igualdad de condiciones en el ejercicio del sufragio, cumpliendo con una misión de interés público.
NECESIDAD DEL TRATAMIENTO	La recopilación y tratamiento de datos personales, incluyendo datos identificativos y especialmente protegidos, es necesaria para: Identificación de Beneficiarios: Verificar que los solicitantes cumplen con los requisitos (discapacidad visual reconocida igual o superior al 33% o afiliación a la ONCE). Gestión del procedimiento: Organizar y proporcionar los recursos necesarios para facilitar el voto accesible (por ejemplo, materiales en Braille, kit de voto accesible). Cumplimiento legal: Adherirse a las disposiciones del Real Decreto 1612/2007 y otras normativas relevantes en materia de accesibilidad y derechos electorales. **Juicio de idoneidad: el tratamiento resulta adecuado para las finalidades.**

EVALUACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD	
PROPORCIONALIDAD DEL TRATAMIENTO	Para evaluar la proporcionalidad, consideramos que el alcance y la naturaleza del tratamiento son adecuados y no excesivos en relación con los fines perseguidos. Este punto se documenta ampliamente en la práctica.
CATEGORÍA DE DATOS RECOGIDOS	Datos Identificativos (DNI/NIF, nombre, dirección, teléfono): Necesarios para asegurar que los materiales, kit de voto accesible lleguen a la persona correcta y para verificar su identidad. Datos Especialmente Protegidos (grado de discapacidad visual, afiliación a la ONCE): Estrictamente necesarios para confirmar la elegibilidad del beneficiario según los criterios establecidos por Ley.
MINIMIZACIÓN DE DATOS	Solo se recopilan datos estrictamente necesarios para cumplir con la finalidad del tratamiento, evitando la recogida de información superflua o irrelevante.
TIEMPO DE CONSERVACIÓN	Los datos se conservan solo durante el tiempo necesario para cumplir con la finalidad del tratamiento y para determinar posibles responsabilidades, conforme a la normativa de gestión documental y archivos aplicable.
ANÁLISIS DE LOS RIESGOS PARA LOS DERECHOS Y LIBERTADES DE LAS PERSONAS AFECTADAS	El tratamiento de datos personales en el procedimiento de "Voto Accesible" presenta ciertos riesgos para los derechos y libertades de los interesados, por ejemplo, en: Protección de datos: Riesgo de acceso no autorizado a datos sensibles. (en todo el ciclo de vida) Integridad: Riesgo de modificación indebida de datos. (ciclo de vida: uso, registro, comunicación) Confidencialidad: Riesgo de divulgación no autorizada de datos. (ciclo de vida: uso-comunicación)
MEDIDAS DE SEGURIDAD	Se implementan medidas de seguridad adecuadas según ENS. ***Medidas de Mitigación ante posibles riesgos encontrados, reforzar o mejorar:*** Controles de acceso: estrictos controles de acceso para asegurar que solo el personal autorizado puede acceder a los datos. Cifrado de datos: tanto en tránsito como en reposo para proteger contra accesos no autorizados. Auditorías: regulares y control de versiones para garantizar la integridad de los datos. Formación del personal: debe ser continua.
CONCLUSIONES	Este previo paso nos permite conocer la idoneidad, necesidad y proporcionalidad del tratamiento de datos. Es probable que nos reunamos con el responsable de seguridad con anterioridad, para ver si esto ya se ha medido, conforme al ENS.

Elaboración propia.

De la figura nº 6 anterior, se ha realizado una simulación a modo de ejemplo. La práctica en el sector público nos indica que es un tratamiento de interés público, además, si ya se ha realizado una EIPD, como parte de su proceso de adecuación al ENS, y este proceso abarca los tratamientos de datos asociados a objetivos de interés público o al ejercicio de poderes públicos, entonces podría considerarse que se ha cumplido con los requisitos del RGPD en relación con la EIPD. En tal caso, no sería necesaria una nueva EIPD separada o distinta bajo las disposiciones del RGPD para esos tratamientos de datos específicos. Otro dato adicional, es que los DPD, de forma proactiva y con otros tipos de tratamientos, continuamos realizando las EIPD en algunas circunstancias. Esto se hace para documentar la inviabilidad de ciertos tratamientos y dejar constancia de la consideración exhaustiva de los riesgos asociados. Aunque la norma general es que, si no se superara la evaluación de necesidad y proporcionalidad, sabemos que podríamos no continuar con la EIPD y si existieran dudas respecto de un tratamiento, incluso tras una EIPD, siempre cabe que se pueda llevar a consulta ante la autoridad de control.

Finalmente, dentro de las funciones organizativas, el DPD, además debe de organizar cómo va a enfocar la respuesta a las solicitudes por el ejercicio de derechos que normalmente se llevan a cabo elaborando sendos Manuales o Protocolos con orientaciones de cómo se gestionará desde que se presente una solicitud hasta dar cierre al seguimiento de la misma. Por otra parte, debe también organizativamente, elaborar el Protocolo de gestión de Brechas de Datos. Aunque la función de "gestión" se recoloca mejor en las funciones de supervisión continua, también se pone sobre la mesa de cara a la organización para trazar las líneas sobre cómo abordar cada fase, desde elaborar el documento tipo; Registro de Incidentes, para la correcta incorporación del incidente que pudiera dar lugar a una brecha de datos, la respuesta ante el incidente, medidas de mitigación, comunicación al departamento técnico o a comités de seguridad, notificación a la autoridad de control, a los afectados y dar seguimiento.

2.3.3. Función de supervisión continua

Sobre la función de supervisión del DPD según las Directrices del GT29 y el RGPD, nos advierten que dicha supervisión no puede ser puntual, sino que ha de ser constante y comprende:

- Recopilación de información constante para identificar actividades de tratamiento.
- Análisis y verificación del cumplimiento normativo de las actividades de tratamiento.
- Proporcionar informes trimestrales, semestrales, anuales con asesoramiento y recomendaciones al responsable o al encargado del tratamiento de datos.

Sobre el cumplimiento normativo, el DPD no es personalmente responsable en caso de incumplimiento; esta responsabilidad recae en el responsable del tratamiento de los datos que es una autoridad pública. Sin embargo, el DPD debe gestionar los riesgos para los derechos y libertades de las personas físicas mediante la identificación, análisis, evaluación, tratamiento y revisión periódica de los riesgos asociados a las operaciones de tratamiento de datos. Estas funciones deben llevarse a cabo de manera continua y actualizarse según sea necesario, especialmente ante cambios en las operaciones de tratamiento de datos de la organización. Como parte de las funciones supervisoras se incluye la actualización por parte del DPD de la normativa vigente en materia de protección de datos o normativa aplicable a la autoridad pública que pueda influir en las operaciones de tratamientos de datos.

Dentro del marco de estas funciones supervisoras también debemos de incluir la gestión de incidentes o brechas de seguridad de datos, así como de su prevención. Esto implica establecer y mantener medidas preventivas y de seguridad adecuadas para reducir el riesgo de ocurrencia de brechas de seguridad. El DPD debe colaborar con otras áreas de la organización para identificar posibles vulnerabilidades en los sistemas y procesos, implementar controles de seguridad efectivos y proporcionar formación y concienciación sobre seguridad de datos a los empleados públicos y todo personal dentro de la Administración. Además, el DPD también puede llevar a cabo evaluaciones de riesgos periódicas y revisar continuamente las políticas y procedimientos de seguridad de datos para garantizar su eficacia y adecuación a las necesidades de la Administración. De otra forma, una vez ocurrido un incidente que, de lugar a una brecha de seguridad de datos personales, tendría que poner en marcha un Protocolo ad hoc para gestionar la brecha de manera adecuada. Esto implica la detección, evaluación y respuesta ante cualquier incidente que pueda comprometer la seguridad de los datos personales. El DPD debe coordinar la respuesta a estos incidentes, asegurándose de que se tomen las medidas reactivas necesarias para mitigar los riesgos y proteger la integridad y confidencialidad de la información. Además, el DPD también puede ser responsable de notificar las brechas de seguridad a la autoridad de protección de datos correspondiente (AEPD) y, en algunos casos, a los interesados afectados, de acuerdo con los requisitos establecidos en el Reglamento General de Protección de Datos.

Las autoridades públicas, los equipos de respuesta a emergencias informáticas (CERT), los equipos de respuesta a incidentes de seguridad informática (CSIRT), los proveedores de redes y servicios de comunicaciones electrónicas y los proveedores de tecnologías y servicios de seguridad pueden tratar los datos personales contenidos en las notificaciones de incidentes de seguridad exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta, adoptando siempre las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo.

Finalmente, se añade a estas funciones supervisoras la de investigar asuntos relacionados con sus funciones, ya sea por iniciativa propia o a petición de la dirección u otros organismos pertinentes, y de informar sobre los resultados de

estas investigaciones a la parte solicitante. El RGPD establece que el DPD debe tener acceso a todos los recursos necesarios, así como a los datos y las instalaciones relevantes para llevar a cabo estas funciones, incluyendo la realización de investigaciones. Además, se espera que tanto el personal interno del responsable de datos como los proveedores externos colaboren plenamente con el DPD en estas investigaciones, proporcionando información completa y respondiendo adecuadamente a sus solicitudes. Es esencial que los responsables de datos establezcan directrices claras para su personal interno y que incluyan cláusulas específicas en los contratos con proveedores externos para asegurar esta colaboración efectiva con el DPD.

2.2.4. Funciones consultivas o de asesoramiento

El DPD puede informar, asesorar y realizar recomendaciones para mejorar las prácticas de protección de datos de la autoridad pública, tanto en relación con el RGPD como con otras legislaciones pertinentes. Además, debe mantenerse actualizado sobre los desarrollos legislativos y normativos en el ámbito de la protección de datos y la seguridad de datos para poder informar adecuadamente. El RGPD requiere que se proporcionen al DPD todos los recursos necesarios y que se fomente su participación en eventos relevantes, como seminarios y conferencias. El DPD también puede ser consultado sobre cuestiones relacionadas con la protección de datos. Es fundamental que la opinión del DPD se tome en consideración en las decisiones con implicaciones en materia de protección de datos, y en caso de desacuerdo, se documenten las razones para no seguir su consejo. Además, el DPD debe ser consultado de inmediato en caso de violación de datos u otros incidentes, y el responsable del tratamiento o el encargado del tratamiento pueden establecer directrices para determinar cuándo debe ser consultado el DPD.

Dentro de las funciones consultivas, se debe de tomar en cuenta el respaldar la implementación de cada uno de los principios de la protección de datos, remarcamos el principio de "protección de datos por diseño y defecto" establecido en el RGPD. Esto implica que el DPD debe ser consultado sobre cualquier asunto relacionado con la protección de datos dentro de la Administración, incluida la elaboración de directrices generales sobre políticas. Este principio requiere que los responsables incorporen medidas técnicas y organizativas apropiadas desde el diseño de sus operaciones de tratamiento de datos, asegurando que se protejan los derechos y libertades de las personas desde un inicio. El DPD debe estar al tanto de los desarrollos legislativos y normativos en este ámbito y brindar orientación sobre cómo implementar este principio en todas las fases del proyecto. Además, el DPD debe asesorar a las administraciones públicas sobre cómo incluir este principio en los contratos públicos y estar involucrado activamente en todas las etapas del diseño, desarrollo y ajuste de proyectos y servicios que puedan vulnerar las normas sobre privacidad y protección de datos.

En este contexto, el DPD debe ofrecer orientación sobre cómo cumplir con las políticas internas de protección de datos, así como garantizar que los contratos y

acuerdos entre diferentes partes involucradas (contratos entre corresponsables del tratamiento, responsable-responsable y responsable-encargados) cumplan con las regulaciones de protección de datos. Además, el DPD debe supervisar el cumplimiento de las Normas Corporativas Vinculantes, que son reglas internas de protección de datos adoptadas por grupos multinacionales, y las cláusulas de transferencia de datos, que establecen los términos para transferir datos personales fuera del Espacio Económico Europeo.

Del mismo modo, El DPD puede recomendar la adhesión a códigos de conducta o certificaciones de protección de datos como medios para demostrar el cumplimiento del RGPD, aunque la decisión final recae en el responsable del tratamiento, en nuestro caso autoridad pública. El DPD también puede colaborar en la obtención de certificados proporcionando información necesaria, pero no puede actuar como perito en sistemas de certificación independientes para evitar conflictos de interés. Aunque los registros detallados de las Evaluaciones de Impacto de Protección de Datos (EIPD) y el seguimiento continuo de las operaciones pueden cumplir funciones similares a las certificaciones, estas últimas tienen la ventaja de ser realizadas por expertos externos e independientes.

Junto a las anteriormente reseñadas funciones, queremos hacer un breve análisis dentro de la estructura de la Estrategia TIC de la AGE, donde podemos atisbar la integración del delegado de protección de datos en coordinación con las unidades TIC de los Ministerios. Dicha coordinación asegura que todas las iniciativas digitales cumplan con la normativa de protección de datos, implementando la privacidad desde el diseño, así como diversas medidas de seguridad. Además, podemos vislumbrar la participación activa del DPD, quien será consultado cuando sea necesario por parte de cada Comisión Ministerial para la Administración Digital (en adelante, CMAD) para garantizar que las políticas digitales consideren la protección de datos desde el inicio y en todas las etapas de los diversos proyectos y planes. Por lo demás, la Secretaría General de Administración Digital, encargada de centralizar las competencias sobre contratación e inversiones TIC, debe trabajar en estrecha colaboración con el DPD. Esta alineación es importante para asegurar que todas las inversiones y contrataciones TIC cumplan con las regulaciones de protección de datos y reflejen buenas prácticas en seguridad y privacidad. Entre las funciones, el DPD también destaca en la supervisión continua del cumplimiento de las normativas de protección de datos dentro del marco de la Estrategia TIC común. Esto incluye la evaluación y mitigación de riesgos relacionados con la privacidad y la protección de datos a lo largo del ciclo de vida de los sistemas de IA y otras nuevas tecnologías digitales.

2.2.5. Funciones de colaboración con la autoridad de control

Por cuanto hasta ahora llevamos dicho, el delegado de protección de datos, como punto de contacto, puede consultar con la AEPD u otras autoridades de control si lo considera oportuno y necesario en el marco de sus obligaciones, así como también

puede ser consultado por la AEPD u otras autoridades de control directamente, en asuntos relevantes. Una realidad es que el DPD debe de cooperar con la autoridad de control cuando sea necesario, esto implica responder a sus solicitudes.

Además, se espera que el DPD participe en la mejora continua de la protección de datos en la institución u organización en la que trabaja, contribuyendo al desarrollo de políticas y procedimientos eficaces. Lo hace, muchas veces atendiendo las diversas pautas que facilita la autoridad de control de ámbito nacional, así como las directrices de otras autoridades autonómicas en el ejercicio de sus competencias. Como ya hemos visto, desde que entró en vigor RGPD con la publicación de diversas Guías para ayudar así al cumplimiento del derecho fundamental a la protección de datos.

2.2.6. Función de gestión de solicitudes y reclamaciones

Los individuos pueden comunicarse con el DPD de una organización para plantear cuestiones sobre el tratamiento de sus datos personales y ejercer sus derechos conforme al RGPD. Esto se facilita mediante la publicación de los datos de contacto del DPD por parte de la organización, como exige el RGPD[7]. La independencia del DPD garantiza que las solicitudes, preguntas o denuncias sean tratadas imparcialmente, sin favorecer ni a la autoridad pública ni al individuo.

Esta función se encuentra relacionada con la función de corte organizativo en cuanto a que es el DPD quién debe de previamente diseñar el protocolo de ejercicio de derechos, para poder cumplir satisfactoriamente la gestión de las solicitudes. El DPD, o los miembros del personal bajo su supervisión, son responsables de gestionar adecuadamente estas solicitudes, brindando respuestas y asesoramiento conforme a la normativa. Si el individuo no queda satisfecho con la respuesta del DPD, tiene el derecho de elevar el asunto a la autoridad de control, AEPD). Este derecho no se ve afectado por la comunicación previa con el DPD. Por lo tanto, los DPD deben estar dispuestos a considerar solicitudes y reclamaciones tanto de personas físicas como de organizaciones representativas.

Visto así, el DPD actúa como un enlace esencial entre el responsable y la autoridad de control, asegurando que la gestión del ejercicio de derechos, se aborden de manera eficaz y justa para todas las partes involucradas. Podemos exponer como plantea el ejercicio de derechos, la política de privacidad de "Mi carpeta ciudadana"[8], nos dice que, se pueden ejercer los derechos en todo momento de

---

7 Podemos revisar ampliamente el Capítulo III, RGPD, Derechos de los interesados. Pero también AEPD, nos facilita ampliamente información para cumplir con la obligación de atender a cada derecho ARSOPOL; acceso, rectificación, supresión ("derecho al olvido"), oposición, portabilidad, limitación del tratamiento, y de no ser objeto de decisiones individualizadas. Revisando en cada derecho un formulario correspondiente para atender las gestiones. Disponible en: https://www.aepd.es/derechos-y-deberes/conoce-tus-derechos/derecho-de-acceso

8 Para ver lo anteriormente mencionado y ampliar la información, pueden visitar la política

forma gratuita, cuando sea responsable del tratamiento; la Secretaría General de Administración Digital. El ejercicio de derechos debe de atenderse por ellos mismos, cuando el ejercicio de derechos corresponda a las categorías de datos que trata; datos identificativos, foto, email, información consultada. Mientras que toda información obtenida a partir de consultas a la Carpeta Ciudadana vía otras Administraciones, toma responsabilidad el órgano responsable en cada caso, pudiendo dirigirse bien al responsable del tratamiento o al DPD designado por cada autoridad pública. Adicionalmente, remarca que le asiste a todo usuario el derecho a presentar una reclamación ante la AEPD.

Precisamente, en lo relativo al derecho personalísimo de acceso en protección de datos, cuestión que aplica para los tratamientos en los que intervenga una IA. Cuando existan decisiones automatizadas, incluida la elaboración de perfiles del art. 22 RGPD, y al menos en tales casos se debe brindar información destacada sobre la lógica aplicada, la importancia y las consecuencias previstas de ese tratamiento para el interesado. Art.15.1 h) RGPD.

Igualmente, el derecho de portabilidad. Quizás no tiene cabida en la mayoría de tratamientos del sector público, pero nos dice que, si el tratamiento de los datos se efectuara por medios automatizado, todo sujeto interesado, deberá recibirlos en un formato de uso común, estructurado, de lectura mecánica para transmitirlo a otro responsable del tratamiento, sin que hubiera algún impedimento. En efecto, esto no se cumple, si el cumplimiento se diera para una misión de interés público o en el ejercicio de poderes públicos.

2.2.7. Función de concienciación y seguimiento

Durante los últimos años, la formación, capacitación o concienciación en materia de protección de datos se ha tornado en un punto esencial para que absolutamente todos quienes conforman o hacen parte del sector público (al igual que en el sector privado), comprendan que este derecho fundamental es fácil de vulnerar y las consecuencias derivadas de una mala gestión relativa a protección de datos pueden ser muy perjudiciales, puesto que los ciudadanos perderían la confianza en el sector público. El rol del DPD parece dividirse en dos aspectos fundamentales respecto de esta función; de una parte, informar al personal sobre sus derechos y responsabilidades en relación con la protección de datos, y de otra capacitar a los responsables y al personal sobre cómo cumplir con estas obligaciones. Esto se logra mediante la creación de conciencia y conocimiento

---

de privacidad del servicio de Mi Carpeta Ciudadana, que es un servicio público, que agiliza la interrelación entre los ciudadanos y las diversas AAPP, pues en dicha carpeta podemos incorporar nuestros datos para que puedan consultarse vía consentimiento, desde los datos educativos, vida laboral, salud, hasta poder realizar otras gestiones; notificaciones, procedimientos, entre otros. Disponible en: https://masinformacioncarpeta.carpetaciudadana.gob.es/infocc/masInformacion.html

interno sobre temas de protección de datos, lo que fomenta un enfoque preventivo más efectivo que uno puramente reactivo.

El DPD implementa medidas como la emisión de comunicaciones informativas para el personal, mediante infografías, recursos educativos, correos electrónicos, así como la organización de sesiones de formación interna y la creación de campañas de sensibilización sobre protección de datos. Es esencial que la información sobre las operaciones de tratamiento de datos sea fácilmente accesible para los interesados a través del sitio web de la organización y otros materiales informativos. Además de la publicación del RAT, políticas de privacidad, se incluyen y adecúan aspectos como el consentimiento y tratamiento de datos a través de cookies, *chatbots* y otros rastreadores en línea, conforme al RGPD y LOPDGDD.

Por tanto, venimos contemplando una serie de tareas o acciones que deberán de estar contenidas en un calendario cronológico de trabajo o cronograma, que desarrolle un plan anual detallado que abarque todas sus responsabilidades y actividades, desde el análisis del contexto inicial, auditorías, pasando por la sensibilización y formación, hasta la gestión de incidentes de seguridad de datos y su seguimiento. Este plan es útil pues le permite al DPD, organizar su trabajo y controlar que las tareas se están cumpliendo de acuerdo a calendario. También gracias a esta planificación puede priorizar acciones, anticipar eventos futuros y contemplar posibles contingencias imprevistas. Igualmente, el DPD revisará y actualizará periódicamente este plan para garantizar su efectividad en la protección de datos en el sector público.

3. NUEVAS FUNCIONES DEL DELEGADO DE PROTECCIÓN DE DATOS POR EL USO DE LA INTELIGENCIA ARTIFICIAL

Estamos inmersos en la constante aceleración y transformación digital, observando la evolución y auge de la Inteligencia Artificial en todos los sectores, especialmente en el sector público, puesto que los ciudadanos esperan mejoras significativas en la gestión de servicios públicos gracias a estas innovaciones tecnológicas que cada vez más acaparan portadas en diversos medios, mostrando sus beneficios, bondades para su puesta en marcha desde la prensa escrita, online[9] hasta las redes sociales.

En esta dirección, observamos como el papel del delegado de protección de datos, adquiere nuevos retos y funciones. Referencia que queda muy difícilmente delimitada en el Nuevo Reglamento de IA, que acaba de entrar en vigor en 2024, pues no crea una nueva figura, pero tampoco atribuye expresamente las competencias en los DPD. Desde la visión práctica, podemos ver que la Inteli-

[9] Microsoft y el Gobierno de España colaborarán en la aplicación de la IA responsable para la mejora de los servicios al ciudadano, el impulso a la innovación, mejora en ciberseguridad nacional y la ciber-resiliencia de las empresas. Disponible en: https://www.computing.es/noticias/microsoft-colaborara-con-el-gobierno-para-implantar-la-ia-en-la-administracion/

gencia Artificial lleva implementada ya hace varios años, sea a través de agentes virtuales, como chatbots. Así como, por ejemplo, el caso de la Junta de Andalucía que implementó una solución de IA, durante la pandemia, para automatizar procesos y poder resolver rápidamente aproximadamente 150.000 solicitudes de subvenciones para trabajadores autónomos. Lo que quiere decir que los DPD ya se encontrarían afrontando funciones por el uso, implementación de inteligencia Artificial. (EY LLP, 2020).

3.1. ¿Qué es la Inteligencia Artificial y cuáles son sus orígenes?

3.1.1. Definiendo a la Inteligencia Artificial

Ciertamente, pudiera creerse un poco fácil de conceptualizar la inteligencia artificial, pero no es así, puesto que ha generado numerosos debates en los últimos años. Desmigándola, por un lado, podemos formular lo que comprendemos por inteligencia, como esa capacidad de entender, comprender, capacidad de resolver problemas, según la RAE, que lo define además como habilidad destreza y experiencia. Mientras que artificial, es producido por el ingenio humano, algo no natural, falso. Actualmente, ya se puede encontrar la definición en la RAE también, como una "disciplina científica que crea programas informáticos para ejecutar operaciones comparables a la que realiza la mente humana, como el razonamiento lógico o aprendizaje".

Desde la visión europea, en el marco de la Estrategia Europea de IA, la Comisión Europea, crea su grupo de trabajo denominado, Artificial Intelligence High-Level Expert Group, que brinda una definición amplia; "Los sistemas de inteligencia artificial (IA) son sistemas de software (y potencialmente también de hardware) diseñados por humanos para actuar en el ámbito físico o digital, con el objetivo de alcanzar una meta compleja. Estos sistemas perciben su entorno mediante la adquisición de datos, interpretan los datos estructurados o no estructurados recopilados, razonan sobre el conocimiento o procesan la información derivada de estos datos, y deciden las mejores acciones a tomar para lograr el objetivo determinado. Los sistemas de IA pueden emplear reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento analizando cómo el entorno se ve afectado por sus acciones anteriores".

De otro lado, el artículo 3 del nuevo Reglamento de IA (en adelante, RIA), define lo que es un **sistema de Inteligencia Artificial**, nos dice que es un sistema basado en máquinas y diseñado para trabajar con distintos niveles de autonomía, pudiendo demostrar gran adaptación después de su despliegue. Adicionalmente para los objetivos que se le requiere, genera predicciones, recomendaciones, decisiones que pueden influir en la vida offline como online. Art.3.1 RIA

Por su parte, leemos a continuación la definición también de "modelo de IA de uso general" se refiere a un sistema de inteligencia artificial que ha sido entrenado con una cantidad significativa de datos utilizando técnicas de autoaprendizaje a gran escala. Este modelo exhibe un nivel considerable de versatilidad y es capaz de desempeñar eficazmente una amplia gama de tareas diversas, sin importar cómo se ponga en circulación en el mercado. Además, tiene la capacidad de integrarse en una variedad de sistemas o aplicaciones adicionales. Es importante destacar que esta definición excluye los modelos de IA utilizados exclusivamente para actividades de investigación, desarrollo o creación de prototipos antes de su lanzamiento al mercado. Art.3.63. RIA

Consecutivamente, el sistema de inteligencia artificial, **basado en un modelo de IA de uso general** es aquel que se fundamenta en un modelo de IA que ha sido entrenado para abordar una amplia variedad de tareas y problemas. Este tipo de modelo de IA de uso general es altamente versátil y puede aplicarse en diversos contextos y para diferentes propósitos. Art.3.65. RIA. Cuando hablamos de un sistema de IA basado en este tipo de modelo, estamos refiriéndonos a un sistema que utiliza dicho modelo como su componente central. Este sistema puede ser diseñado para realizar una tarea específica, como reconocimiento de voz, clasificación de imágenes o análisis de datos, entre otros. Sin embargo, debido a la versatilidad del modelo de IA de uso general en el que se basa, el sistema puede adaptarse y utilizarse para una variedad de propósitos y aplicaciones. En cierta medida, este sistema de IA no solo puede ser utilizado de manera independiente para llevar a cabo tareas específicas, sino que también puede integrarse en otros sistemas de IA más complejos o en aplicaciones más amplias. Por ejemplo, podría incorporarse en un sistema de procesamiento de lenguaje natural para mejorar la capacidad de comprensión y respuesta del sistema.

En dicha línea el grupo de expertos para intentar de dar forma a todo lo que engloba IA y así situarnos, indican que, "la IA es una disciplina científica, dentro de la informática, que abarca varios enfoques y técnicas, a) como el aprendizaje automático o machine learning, que incluye el aprendizaje profundo o Deep learning y el aprendizaje por refuerzo, b) el razonamiento automático o machine reasoning, que abarca planificación, programación, representación y razonamiento del conocimiento, búsqueda y optimización y c) la robótica, que incluye control, percepción, sensores y actuadores, así como la integración de todas las demás técnicas en sistemas ciberfísicos." Comisión Europea, 2019.

Figura 7. Definiciones del Reglamento de Inteligencia Artificial

Elaboración propia basada en el RIA para el Seminario de IA del Máster Universitario en Derecho Digital de UNIR.

3.1.2. Orígenes de la Inteligencia Artificial

En lo que respecta a la historia podemos atisbar que la IA no es algo reciente, tiene sus raíces en la década de 1940–1950, y mencionaremos algunos especiales hitos que han marcado el recorrido hasta hoy. Warren McCulloch y Walter Pitts publicaron un trabajo en 1943 que describía un modelo matemático de redes neuronales artificiales, estableciendo una base conceptual para el desarrollo de la IA (McCulloch y Pitts, 1943). En 1950, Alan Turing publicó "Computing Machinery and Intelligence", donde introdujo el Test de Turing, un criterio para determinar si una máquina puede exhibir un comportamiento inteligente indistinguible del de un humano (Turing, 1950).

En 1956, la conferencia de Dartmouth, organizada por John McCarthy, Marvin Minsky, Nathaniel Rochester y Claude Shannon, se reconoce como el evento fundacional de la IA como campo de estudio. En esta conferencia, John McCarthy acuñó el término "Inteligencia Artificial" (Russell y Norvig, 2021). En 1957, Frank Rosenblatt desarrolló el perceptrón, una red neuronal capaz de aprender a través del entrenamiento, marcando un avance significativo en el aprendizaje

automático (Rosenblatt, 1957). En 1965, Joseph Weizenbaum creó ELIZA, uno de los primeros programas de procesamiento de lenguaje natural capaz de simular una conversación con un psicoterapeuta (Weizenbaum, 1966). Durante esta década, el campo de la IA se consolidó formalmente, pues también nace el primer autómata con movimiento denominado Shakey, su creador Charles Rosen evitó que se le denominara robot, pero hoy resulta todo un pionero por combinar planificación, modelado y aprendizaje, pues fue el primer robot inteligente y la industria de los coches o videojuegos aún conservan sus bases.[10]

Mientras que, la década de 1970 estuvo marcada por un periodo conocido como el "invierno de la IA", caracterizado por una disminución del interés y la financiación debido a las altas expectativas no cumplidas y a las limitaciones técnicas de la época (Russell y Norvig, 2021). No obstante, durante este tiempo se desarrollaron sistemas expertos como MYCIN, diseñado para diagnosticar infecciones bacterianas y recomendar tratamientos adecuados (Shortliffe, 1976). Parece importante mencionar también que aparece el Revenue Management en 1972, cuando Kenneth Littlewood presentó un modelo matemático con el que calcular la previsión de las reservas de los billetes de avión, sistema que fue ampliamente utilizado primero en la industria de la aviación y que luego se compartió en la industria Hotelera. (Hosteltur, 2016). Hoy en día este sistema de gestión de ingresos continúa vigente en muchos sectores y mejorado, realiza análisis predictivos y algoritmos para optimizar los precios y la disponibilidad de productos o servicios con el fin de maximizar los ingresos. Los sistemas de Revenue Management utilizan algoritmos sofisticados para analizar grandes cantidades de datos y generar recomendaciones sobre precios óptimos, disponibilidad de inventario y estrategias de distribución.

10 años más tarde, la IA experimentó un resurgimiento del interés, en la década de 1980, especialmente en el desarrollo de sistemas expertos que capturaban el conocimiento humano en reglas lógicas (Russell y Norvig, 2021). En 1986, Geoffrey Hinton, David Rumelhart y Ronald Williams redescubrieron y popularizaron el algoritmo de retropropagación, fundamental para el entrenamiento de redes neuronales profundas (Hinton, Rumelhart y Williams, 1986). La década de 1990 presenció avances significativos, incluyendo la victoria de Deep Blue de IBM sobre el campeón mundial de ajedrez Garry Kasparov en 1997, demostrando la capacidad de las máquinas para superar a los humanos en tareas complejas y específicas (Campbell et al., 2002).

Posteriormente la IA comenzó a integrarse en aplicaciones comerciales como motores de búsqueda en los años 2000, asistentes personales digitales y sistemas de recomendación (Russell y Norvig, 2021). En 2006, Geoffrey Hinton introdujo el

---

[10] Se puede conocer el prototipo de Shakey, conocido hoy como el primer robot inteligente a nivel mundial, así como su historia, en el artículo escrito por Sánchez, C. 2017 para el Diario. es en https://www.eldiario.es/hojaderouter/tecnologia/shakey-robot-inteligencia-artificial-coche-autonomo_1_3466717.html

concepto de "aprendizaje profundo" (deep learning), utilizando redes neuronales con múltiples capas para modelar representaciones jerárquicas de datos (Hinton et al., 2006). La década de 2010 marcó un avance notable en el campo de la IA. En 2011, Watson de IBM ganó el concurso Jeopardy, demostrando capacidades avanzadas en procesamiento de lenguaje natural y búsqueda de información (Ferrucci et al., 2010). En 2012, AlexNet, una red neuronal convolucional, ganó la competición ImageNet, superando significativamente a otros métodos en el reconocimiento de imágenes (Krizhevsky et al., 2012). En 2014, Google adquirió DeepMind y su sistema AlphaGo venció a campeones humanos de Go en 2016, un juego considerablemente más complejo que el ajedrez (Silver et al., 2016).

La IA en la década de 2020 trae avances en IA generativa, como GPT-3 de Open AI (hoy ya con GPT 4) demostraron capacidades impresionantes en generación de texto y procesamiento de lenguaje natural (Brown et al., 2020). Además, se observó una mayor integración de la IA en áreas como la salud, la automoción con vehículos autónomos, la robótica y la industria. La IA continúa evolucionando con investigaciones en áreas como la ética y la gobernanza de la IA y la mejora continua de algoritmos de aprendizaje automático y redes neuronales. El desarrollo de una Inteligencia Artificial General, una inteligencia que puede realizar cualquier tarea cognitiva que un ser humano puede, sigue siendo un objetivo a largo plazo con importantes desafíos técnicos y filosóficos (Russell y Norvig, 2021).

3.2. Inteligencia artificial en el sector público

Para remarcar la importancia del Sector Público en la vida de un ciudadano partimos que los poderes públicos legitiman a la Administración quién debe de velar por el bienestar de los ciudadanos al igual que debe de hacer todo lo posible por cuidar de sus derechos fundamentales. Sin embargo, cuando llega una nueva tecnología que puede tomar decisiones arbitrarias mediante sus algoritmos, resulta interesante que tome diversas actuaciones. De ahí que actualmente se hable de 3 roles que ejercería, el primero de ellos se encuadra desempeñando la creación de bases normativas, de otra parte, el segundo rol se erige como un impulso que se acelera gracias a las propuestas de creación de diversos proyectos en materia de IA y que veremos más adelante como se están organizando grandes presupuestos. El tercer rol, que hasta ahora ha sido el menos importante de los anteriores y en breve tomará más importancia, se bifurcaría en el papel del sector público como desarrollador y usuario[11] de Sistemas de IA. Gamero Casado (2023) pag, 76.

---

[11] Es importante remarcar que RIA así como otros autores, nos hablan de "usuario" o "usuarios", pero no podemos entender al usuario como el titular de los datos personales (interesado, afectado), sino como "las entidades que usan los sistemas de IA" (Cotino Hueso, 2022). Es fácil de confundirse a través de la lectura y por ello se necesita hacer un estudio profundo y muy pormenoriza-

3.2.1. Casos de uso de IA actuales en el sector público

En los últimos años, observamos cómo el sector público está adoptando cada vez más la inteligencia artificial, para mejorar la eficiencia a través de la mejora de procesos y acelerar la efectividad de los servicios públicos a través de la fácil interacción y adopción de soluciones a los problemas que enfrenta la población en su día a día, gracias a la innovación que también se plantea como un pilar básico para dar vida a la IA en las AAPP. Lo cierto es que las demandas y necesidades de los ciudadanos exigen una mayor capacidad de respuesta y personalización de los servicios públicos, junto con crecientes expectativas sobre el papel de la Administración en la era digital.

Si echamos un vistazo a los informes o los datos abiertos de Public Sector Tech Watch (en adelante, PSTW), que es un observatorio del uso de tecnologías emergentes, podemos ver los casos de uso a nivel europeo y si nos acercamos a España, podemos observar los 82 proyectos, de los cuales 61 son sólo de IA(y cada día van en aumento, se puede comprobar tras esta publicación que la cifra habrá incrementado). Visto esto, reconocemos que es esencial avanzar hacia un sector público tecnológicamente avanzado, donde la IA y el análisis de grandes volúmenes de datos sean elementos clave para enfrentar las necesidades de la sociedad en general. España se encuentra en una posición favorable en este ámbito, ocupando el sexto lugar entre los países de la UE en la implementación de algoritmos en el sector público. (Ministerio de Transformación Digital, 2024. Pág. 42)

Hablando en términos generales, revisamos de nuevo el visor donde vemos implementados totalmente 30 proyectos, en modo prueba o como proyectos piloto hay un total de 24, en cambio 3 de ellos ya no están en uso, *como COVID19 Aragón Bot*, *Well co* y *servicio 060* respuestas y preguntas sobre tramitaciones. Entre los proyectos de IA actuales tanto implementadas como en piloto, podemos observar de forma general que incluyen:

a) Automatización de procesos administrativos: La IA se utiliza para automatizar tareas administrativas rutinarias, reduciendo la carga de trabajo manual y con ello pretende aumentar la eficiencia operativa. Como ejemplos tendríamos*; EMI para el Servicio Público de Empleo de Galicia* para sincronizar la oferta y demanda de empleo, IA para la decisión y ayuda en procesos en los servicios sociales de Barcelona. Ahora bien, el Ayuntamiento de Barcelona, ha aprobado un protocolo que garantice el uso ético de los servicios digitales cuando usen IA.[12]

b) Análisis de datos y toma de decisiones: Los sistemas de IA analizan grandes volúmenes de datos para identificar patrones y tendencias, apoyando

---

do del nuevo Reglamento (RIA) para no caer en interpretaciones que nos lleven a crear confusión.

[12] Protocolo que se torna en un punto de partida o como en el mismo se aprecia como; "documento pionero que aborda la gobernanza de los sistemas algorítmicos de ámbito local" Disponible en: https://bci.inap.es/alfresco_file/1e08c381-8af2-451a-9102-70f4c061994e

la toma de decisiones basadas en datos en áreas como la planificación urbana, la salud pública y la seguridad. Aquí podemos encontrar del PSTW, *DATAESTUR*, que realiza análisis de datos de turismo y facilita mucha información en abierto. También podemos mencionar el monitoreo de la capacidad de la playa de Calella para controlar el aforo mediante drones e IA que avisa a los agentes municipales para que puedan limitar el aforo, creando así mayor seguridad a los ciudadanos.

c) Mejora de servicios al ciudadano: Los chatbots y asistentes virtuales basados en IA proporcionan atención al cliente y soporte a los ciudadanos, mejorando la accesibilidad y la calidad de los servicios públicos. *Arantxat*, es otro ejemplo, una Guía turística virtual de Guipuzkoa, desarrollada bajo un sistema chatbot disponible para WhatsApp que incluye las consultas más habituales recibidas en las oficinas de turismo. De otra parte, tenemos a *Línea Madrid chat online*, asistente virtual que brinda información sobre gestiones varias como agendar una cita previa, solicitar certificado de empadronamiento, entre otros.

   Uno de los casos que ha tomado mayor importancia es el de la Agencia Tributaria que ha colaborado con *IBM Watson* para implementar un asistente virtual basado en inteligencia artificial destinado a resolver consultas relacionadas con el suministro inmediato de información del IVA (IBM.2018). Esta iniciativa ha tenido un impacto significativo, con una reducción del 80% en el número de correos electrónicos recibidos y un aumento diez veces mayor en las consultas al asistente virtual durante la primera semana. Además, se ha observado un fomento del cumplimiento tributario, ya que la IA permite detectar situaciones irregulares y disuadir a los contribuyentes de continuar con prácticas no conformes. Por ejemplo, la Agencia Tributaria ha enviado comunicaciones a pequeñas empresas informándoles que, según la información obtenida a través de IA, sus ingresos declarados están por debajo de la media del sector.

   Para la mejora de los servicios en el ámbito de la salud, vemos varios proyectos en Madrid, como *Faith*, monitoreo de la salud mental con IA, del Hospital Gregorio Marañón y en el Hospital Clínico San Carlos Madrid, IA creada para salvar la vida de los pacientes psiquiátricos. De otra parte, en Hospital Miguel Servet de Zaragoza, vemos *Track Ai,* para ayudar a detectar signos tempranos de discapacidad visual.

d) Seguridad y vigilancia: se emplea la IA, en sistemas de vigilancia y seguridad para detectar comportamientos sospechosos y prevenir delitos, utilizando técnicas de reconocimiento facial y análisis predictivo. A día de hoy vemos que continúa activo *VERIPOL*, el sistema que sirve para ayudar a identificar o detectar denuncias falsas. Cabe mencionar *Viogen*, que realiza pronóstico de casos de violencia de género. Reconocimiento facial y de documentos oficiales para proporcionar identidades digitales, en la que viene trabajando

AOC, Administració Oberta de Catalunya, ya en 2016 crearon *IdCAT Móvil*, ahora ha incorporado VERIDAS y varias mejoras en la aplicación.

Figura 8. Datos en abierto, del visor de casos y estadísticas de uso de IA en el sector público

Fuente: Public Sector Tech Watch. Revisado en abril de 2024. Disponible en: https://joinup.ec.europa.eu/collection/public-sector-tech-watch/cases-viewer-statistics

3.2.2. Estrategia Nacional de inteligencia Artificial 2024

Recientemente, fruto también de la implementación de la Estrategia Europea de IA, se ha aprobado la Estrategia Nacional de Inteligencia Artificial 2024[13]. Esta estrategia considera a la IA una palanca de crecimiento económico, técnico y social, debido a su alto impacto y auge. La Estrategia nace en 2020 del Plan de Recuperación, Transformación y Resiliencia (en adelante, PRTR) cuando indicaba que creía necesario impulsar una digitalización humanista que se alineara con la Carta de Derechos Digitales. con un presupuesto de 1.500 millones de

[13] El Plan de Recuperación abordaba el desarrollo de siete planes estratégicos que desarrollan la agenda España Digital 2025: el Plan de Digitalización de las Administraciones públicas, el Plan de Conectividad, la Estrategia Nacional de Inteligencia Artificial, la Estrategia de Impulso 5G el Plan Nacional de Competencias Digitales, el Plan de Digitalización de las pymes y el Plan España Hub Audiovisual de Europa. Estos objetivos, en consonancia con la Estrategia Digital para Europa.

euros adicionales a los 600 millones previos, busca expandir el uso de la IA en la economía y la administración pública durante 2024 y 2025.

Una de las principales conclusiones mencionadas es respecto del despliegue de la IA, que requiere de una permanente colaboración público-privada a la vez que de un amplio y común consenso social en torno al diseño de los procesos de decisión. La Estrategia de Inteligencia Artificial 2024 viene trabajando en tres ejes de actuación y varias palancas, que resumimos:

a) Primer eje para reforzar las capacidades para el desarrollo de la IA:
   - Supercomputación: se prevé la inversión de 90 millones de euros en nuevos clústeres y en mejorar la Red Española de Supercomputación (RES) creado en 2007, dedicando un 20% de la capacidad del Mare Nostrum 5 para la industria.
   - Modelos de lenguaje: Desarrollo de modelos de lenguaje en castellano y lenguas cooficiales, llamados ALIA.
   - Almacenamiento sostenible: Creación de Centros de procesamiento de datos sostenibles con un nuevo marco regulatorio.
   - Impulso al talento: Inversión en becas y formación, 120 millones de euros, y 30 millones de euros en proyectos específicos para IA. En el Sector público se es consciente que se necesitará contar con nuevas generaciones de funcionarios altamente cualificados y con gran capacidad de adaptación, por lo que se propone la creación de un nuevo modelo en el ámbito de la función pública.

b) Segundo eje para facilitar la aplicación de la IA en el sector público y privado:
   - GobTech Lab: Innovación en la Administración General del Estado mediante proyectos piloto que se pondrán a prueba en un laboratorio de innovación. Para esto se crea un proceso desde las propuestas del caso de uso en una AAPP, dando prioridad a proyectos más importantes, desarrollándolo a continuación para su posterior evaluación de conformidad por parte de AESIA.
   - Kit Consulting y Kit Digital: Programas para apoyar la adopción de IA en pequeñas y medianas empresas, con una inversión total de 650 millones de euros.
   - Fondo Next Tech: 400 millones de euros para financiar empresas que desarrollen soluciones de IA. Se propone un Plan de despliegue mediante la creación de una plataforma donde se puedan desarrollar pruebas de concepto y también la creación de Espacio de datos de la Lengua, para desarrollo de aplicaciones y diversos modelos de lenguaje. Se incluye aquí la ayuda a *startups* para facilitar su crecimiento.
   - Nueva Ley de Ciberseguridad: se pretende crear un marco integral y claro para mejorar la ciberseguridad y proteger sistemas de infor-

mación. Actualmente resulta imprescindible fortalecer la ciberseguridad, esto además se hace eco y resulta un desafío cuando además se ve el gran impacto de la IA en la ciberseguridad.

c) Tercer eje para fomentar una IA ética transparente y humanística:
   - La Agencia Española de Supervisión de la Inteligencia Artificial (AESIA): tomará protagonismo, actuará como centro de pensamiento y análisis, supervisor del despliegue responsable de la IA, y referente internacional en gobernanza de IA.

La Secretaría de Estado de Digitalización e Inteligencia Artificial coordinará la estrategia, con la participación de todos los Ministerios a través de la Comisión Interministerial. Esta comisión se encargará del seguimiento de las medidas y del informe de las distintas fases de la Estrategia.

3.3. Implicaciones de la IA en la protección de datos

La Unión Europea, con "AI Act", "Reglamento IA" o "Ley de IA", busca establecer un nivel de protección coherente y compacto en toda su jurisdicción. El objetivo es asegurar el desarrollo de una Inteligencia Artificial confiable y, al mismo tiempo, imponer obligaciones uniformes para todos los operadores que utilicen, importen o desarrollen sistemas de IA.

Pero ¿cuál es el impacto de esta nueva tecnología en el ámbito de la protección de datos? Es relativamente fácil deducir que la IA requiere de grandes volúmenes de datos para entrenar y optimizar sus modelos. Este proceso de recolección de datos, plantea grandes desafíos en protección de datos tal y como lo vemos cuando se emplean técnicas de *Big data*. Para no vulnerar este derecho fundamental, tenemos que partir por aplicar los principios de la protección de datos que nos van a guiar hacia un cumplimiento, además en términos éticos, esto quiere decir que al recopilar gran cantidad de datos debemos de procesar aquellos que resulten estrictamente necesarios (principio de minimización). Los datos que harán parte del entrenamiento de la IA, deben de ser recogidos con fines específicos, explícitos y legítimos (principio de limitación), a su vez, deben ser lícitos, leales y transparentes, esto implica, informar claramente a los individuos sobre cómo se utilizarán sus datos y obtener su consentimiento cuando sea necesario (principio de licitud, lealtad y transparencia). En función a la legalidad, es importante considerar que algunas bases jurídicas, como el interés legítimo, no pueden ser utilizadas por las Administraciones Públicas como hemos ido viendo en algunos apartados (salvo que no actúen en ejercicio de funciones estrictamente públicas). Por tanto, esto no impide que las AA.PP. usen un sistema de IA desarrollado por un tercero que haya utilizado esa base jurídica. Lo que no pueden hacer las AA.PP. es usar esa misma base jurídica para justificar tratamientos posteriores de datos, tendrá el DPD junto con el responsable del tratamiento velar que los nuevos tratamientos tengan una base de legitimación

adecuada. Como sabemos, la elección de las bases jurídicas está directamente relacionada con la finalidad del tratamiento y con las competencias atribuidas a las AA.PP. Todo lo anterior sería aplicable si realmente hubiera un tratamiento de datos. No obstante, y recordando el anterior número de esta revista, donde hablábamos de Espacios de Datos, es común que las Administraciones públicas, utilicen estos espacios para volcar la información de diversas fuentes, dicho así, utilizan datos que son denominados estructurados, recopilados o extraídos de fuentes, como datos censales, estadísticos y que ya no son considerados datos personales porque nunca lo han sido o han sido anonimizados.

En lo relativo a transparencia, podemos obtener grandes referencias y facetas de Cotino Hueso 2022, pág. 25-70, quién hace un estudio amplio sobre la transparencia y explicabilidad, encuadrando la transparencia como externa e interna, esta última se toma en cuenta desde el punto de vista normativo y la primera desde las garantías de los derechos constitucionales principios y valores. Después de este paréntesis, vemos como el RIA se enfoca en asegurar que los usuarios intervinientes comprendan, sean conscientes y utilicen adecuadamente los sistemas de IA y durante todo el ciclo de vida de esta nueva tecnología, por ejemplo, asegurando proveedores, implementadores que informen sobre; instrucciones de uso, documentación sobre sus capacidades y limitaciones, garantizando así la trazabilidad y explicabilidad de los mismos, igualmente, se informará a las personas afectadas de sus derechos (RIA, considerando 27). Mientras que la transparencia del RGPD se centra en proteger los derechos de las personas físicas mediante la información clara y accesible sobre el tratamiento de sus datos personales. El considerando 67 RIA, indica que, para cumplir con el RGPD y otras normativas de la UE, es esencial que la gestión de datos personales sea transparente sobre el propósito original de su recolección. Incluso debe de informarse a los interesados, si es posible que su información pueda ser reidentificable o no, si se cruzan diversos conjuntos de datos, en las etapas de entrenamiento del sistema de IA. Refuerza la necesidad de que, para cumplir con el RGPD y otras normativas de la UE, sea esencial que la gestión de datos personales sea transparente sobre el propósito original de su recolección. Los conjuntos de datos deben ser estadísticamente adecuados y prestar especial atención a evitar sesgos que puedan perjudicar la salud, la seguridad o los derechos fundamentales de las personas, o resultar discriminatorios. Esto es fundamental, especialmente cuando los resultados de la IA influyen en futuras entradas de datos, creando retroalimentación.

Continuando, en términos de principios, los datos personales dentro del sistema de IA, deben conservarse de forma que permita la identificación de los interesados, durante el tiempo necesario para los fines del tratamiento. (principio de limitación del plazo de conservación), Adicionalmente, se requiere que todos los datos sean exactos y actualizados, tomándose las medidas oportunas para garantizar que cualquier dato inexacto se suprima o rectifique. (principio de exactitud). Los datos personales además deben ser tratados para que se custodie

y garantice una seguridad adecuada, de forma que no se modifiquen, roben, deterioren, destruyan o pierdan (principio de integridad y confidencialidad) añadiendo además el principio de responsabilidad proactiva que nos dice que todo responsable del tratamiento debe ser capaz de demostrar que se cumple con estos principios durante todo el ciclo de vida de los datos, al igual que en todo el ciclo del sistema de IA.

El considerando 45 bis, que tras los diversos borradores hoy es el considerando 69, refuerza lo dicho anteriormente para que se cumpla con la ética y buenas prácticas; cuando afirma que el derecho a la intimidad y a la protección de los datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. Pues vemos grandes similitudes en contraposición al ciclo de vida de los datos de las personas físicas. A este respecto, continúa el RIA, que los principios de minimización de datos y de protección de datos desde el diseño y por defecto, son aplicables cuando se tratan datos personales. Por tanto, las medidas adoptadas por los proveedores para garantizar el cumplimiento de dichos principios pueden incluir no solo la anonimización y el cifrado, sino también el uso de tecnología que permita llevar algoritmos a los datos y permita el entrenamiento de los sistemas de IA sin la transmisión entre las partes o la copia de los propios datos en bruto o estructurados, sin perjuicio de los requisitos sobre gobernanza de datos previstos en el RIA.

Figura 9. Cuestiones relevantes del Reglamento de Inteligencia Artificial

Elaboración propia basada en el RIA. para el Seminario de IA del Máster Universitario en Derecho Digital de UNIR.

Ahora veremos cuáles son los roles dentro de los sistemas de IA, partimos por las definiciones del artículo 1 RIA, siendo difícil contextualizarlo dentro de los roles del RGPD, puesto que cada sistema de IA, puede tener sus particularidades, salvedades y también dependerá si se tratan o no datos personales. Una vez dicho esto, pensamos que el Comité de IA debe de documentar vía informes y en cada sistema de IA utilizado, la atribución de los roles para que todo el equipo vaya en la misma dirección:

- **Proveedor:** Es la persona física o jurídica, autoridad pública que desarrolla un sistema de IA o un modelo de IA de uso general y lo introduce en el mercado. En el contexto del RGPD, el proveedor podría ser comparable al responsable del tratamiento si determina los fines y medios del tratamiento de datos personales. Sin embargo, si el proveedor actúa únicamente bajo las instrucciones de otro ente, podría considerarse un encargado del tratamiento.
- **Responsable del despliegue:** Es la autoridad pública, persona física o jurídica que utiliza un sistema de IA bajo su propia autoridad. Puede compararse con el responsable del tratamiento del RGPD cuando el responsable del despliegue determine los fines y medios del tratamiento de datos personales mediante el sistema de IA.
- **Distribuidor:** Esta persona forma parte de la cadena de suministro y comercializa un sistema de IA en el mercado de la Unión Europea. también puede tener responsabilidades relacionadas con el tratamiento de datos si está involucrado en la distribución de sistemas que tratan datos personales y podría ser un encargado del tratamiento si actúa bajo las instrucciones del responsable del tratamiento.
- **Importador:** Es quién introduce en el mercado un sistema de IA fabricado por una entidad establecida en un tercer país. Está relacionado con la entrada de productos al mercado europeo, lo cual puede implicar el tratamiento de datos personales. Podría ser un encargado del tratamiento si maneja datos personales bajo las instrucciones del responsable del tratamiento.
- **Representante autorizado:** Es una persona física o jurídica, autoridad pública, que actúa en nombre del proveedor para cumplir con las obligaciones establecidas en el Reglamento de IA. Podría ser equiparable a un representante legal que actúa en nombre del responsable del tratamiento.
- **Operador:** Este término abarca a varios roles involucrados en diferentes etapas del ciclo de vida de un sistema de IA, incluidos proveedores, fabricantes del producto, responsables del despliegue, representantes autorizados, importadores y distribuidores. En el contexto del RGPD, cada uno de estos roles puede tener responsabilidades específicas en relación con el tratamiento de datos personales que habrá que distinguir llegado

el momento y en cada caso específico. En ningún caso sería aceptable derivar la responsabilidad al propio sistema IA. (AEPD.2020)

3.4. Nuevas funciones para los delegados de protección de datos

Conforme hemos visto hasta aquí, apreciamos que el delegado de protección de datos deviene en una figura fundamental que ya viene abordando, quizás de forma muy escalonada, la integración de la IA, así como su uso en el seno de las administraciones públicas, (y también en las entidades privadas). Pues como hemos visto hasta ahora, la Inteligencia Artificial viene desarrollándose e implementándose con fuerza en al menos los últimos 4-5 años.

El DPD desempeña un papel importante al facilitar la comunicación de información a los interesados sobre el desarrollo, mantenimiento y explotación de sistemas de IA utilizados en procesos de tratamiento de datos. Si bien el Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, establecen las condiciones para la designación de un DPD, como hemos visto en el apartado 2. El Reglamento de IA, tampoco implementa una nueva figura como el IA Officer o Chief Artificial Intelligence Officer, ni atribuye las competencias en los DPD. Para abordar esta cuestión, por ejemplo, la Confederación de Organizaciones Europeas de Protección de Datos, CEDPO, venía desarrollando encuestas para conocer nuestra conformidad como DPD, por si estuviéramos de acuerdo en asumir las funciones en lo que respecta a IA, si ya las estamos asumiendo, o si consideramos que debe asumirla otra figura, desde luego es una encuesta que resulta interesante para saber cuál es la situación real de los DPD en el marco de los tratamientos de la IA y sentirnos escuchados. Consecutivamente en meses posteriores nos brindó respuesta a la interrogante sobre si el DPD es la figura adecuada para participar en el rol de oficial de IA, indicando que se presentan desafíos en lo relativo a:

1. Conflicto de Intereses: El artículo 38 del RGPD restringe que el DPD supervise actividades de cumplimiento cuando también participa en la implementación directa de sistemas de IA, ya que esto comprometería su independencia.
2. Independencia del DPO: La autonomía del DPO podría verse comprometida si asumiera responsabilidades en la implementación de IA, ya que esto podría diluir sus funciones de supervisión.

Destacando además que, en las entidades más pequeñas, donde los presupuestos son limitados, es común que varias funciones y roles recaigan en una sola persona. Esto también ocurre en el ámbito público, mientras que la administración central cuenta con un presupuesto mayor para invertir en soluciones de IA, las administraciones autonómicas y locales enfrentan restricciones económicas que dificultan la adquisición de estas tecnologías,

las cuales suelen ser costosas. Berning Prieto (2023) Además el Centro de Transferencia de Tecnología podría representar un apoyo importante para las entidades locales al igual que lo serán los entornos controlados de pruebas o *Sandbox* de IA.[14] Que se van a impulsar, así como las grandes partidas presupuestarias que ya se prevén en ENIA. Esperamos que la figura del DPO también se considere como una palanca más dentro de la estrategia y partida presupuestaria.

Sobre la designación de un DPD, la observación habitual y sistemática a gran escala o el tratamiento de categorías especiales de datos, según el RGPD, pueden determinar la necesidad de contar con un DPD. Según las Directrices sobre los delegados de protección de datos, el DPD se torna en una figura importante de cara al cumplimiento y la gestión de riesgos para los derechos de los interesados. Por lo tanto, aunque no sea obligatorio en los casos de IA que tengan asignado un riesgo más limitado o mínimo (Aunque podemos revisar que hasta para los *chatbots* de riesgo limitado se prevé un cumplimiento riguroso a efectos de transparencia, AEPD ha emitido como debe cumplirse con el deber de información y transparencia).

El DPD resulta extremadamente útil y necesario para entidades que utilizan IA en el tratamiento de datos personales o desarrollan soluciones de IA que requieren datos personales para el entrenamiento de los modelos. En particular, el DPD se identifica como un elemento clave desde la privacidad desde el diseño y por defecto, en la realización de Evaluaciones de Impacto en la Protección de Datos (EIPD) y como una herramienta esencial para implementar la transparencia RGPD-RIA.

Para poder comprender todas las funciones que ya lleva desempeñando un DPD, primero deberíamos de posicionarnos en el contexto de la entidad, realizar un inventario de la IAs. Es decir, los sistemas de IA que se quieran implementar o proyectos que ya se están ejecutando. Bien sabemos que el DPD es experto en crear sus propias arquitecturas de cumplimiento (un Sistema de Gestión de Privacidad de la Información o SGPI por ejemplo basada en ISO/IEC 27701 o participar en la gestión y puesta en marcha de otros estándares internacionales como el SGSI vía ISO/IEC 27001, por lo que aparece en este horizonte un nuevo *framework*, ISO/IEC 42001:2023 es la primera norma sobre sistemas de gestión de IA (SGIA) que nos ayuda a un uso de IA responsable, estableciendo directrices claras para la gobernanza de la IA, la gestión de riesgos, la trazabilidad, la

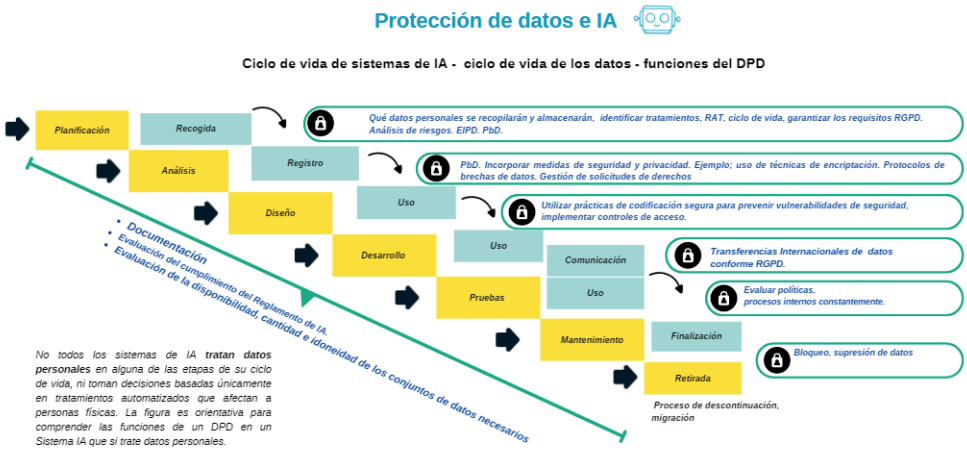
---

[14] El Sandbox es una iniciativa impulsada por la Secretaría de Estado de Digitalización e Inteligencia Artificial, que ofrece a las organizaciones participantes la oportunidad de experimentar de forma práctica y realista cómo aplicar el Reglamento europeo de Inteligencia Artificial en sus sistemas. Con asistencia técnica personalizada y capacitación, las empresas podrán probar la implementación de estos requisitos con apoyo especializado. El sandbox está abierto a sistemas de IA de alto riesgo, así como a sistemas de propósito general y modelos fundacionales, cuando se considere que tienen potencial para un uso de alto riesgo.

transparencia y la confiabilidad, además de promover un aumento de la eficiencia. Proporcionando un marco estructurado que permite a las organizaciones implementar y mantener sistemas de IA que respeten principios éticos y legales, asegurando que las aplicaciones de IA sean seguras, efectivas y confiables. La ISO/IEC 42001 también fomenta la adopción de prácticas de IA que se alineen con los objetivos estratégicos de las organizaciones, facilitando la integración de la IA en sus procesos operativos y de toma de decisiones de manera sostenible y responsable.

Como segundo punto, debería de contemplarse el ciclo de vida de un Sistema de Inteligencia Artificial, vemos como en paralelo podemos hablar sobre el ciclo de vida de los datos personales, para entender mejor el porqué es importante el papel que desempeña un DPD, de forma que el ciclo de vida de un sistema de IA comprende etapas desde la conceptualización y diseño hasta la implementación, mantenimiento y retirada, mientras que el ciclo de vida de los datos personales abarca desde su recopilación y almacenamiento hasta su uso, eliminación o anonimización. En este punto, el DPD juega un papel decisivo, debido a sus conocimientos, para asegurar que, en cada etapa del ciclo de vida de los datos personales, en caso de haber tratamientos de datos, se cumplan con las normativas de protección de datos, garantizando así la privacidad y seguridad de la información. En tal caso, es verdad que no todos los sistemas de IA incorporan el tratamiento de datos personales en alguna fase de su desarrollo, ni se basan exclusivamente en procesos automatizados que incidan directamente a personas físicas. La referencia a la figura 10 es útil para ver como se ve en paralelo ambos ciclos de vida y comprender las responsabilidades que este tendría en un Sistema de IA que efectivamente trate datos personales. Adicionalmente, hay que tomar en cuenta que pueden existir más de un ciclo de vida de los datos en los sistemas de IA. La UNE-EN ISO/IEC 8183:2024 nos confirma que, en el campo de los sistemas de IA, se prevén varios riesgos, pues existen muchos ciclos de vida de los datos en uso y bajo consideración para diferentes propósitos como pueden ser la calidad de los datos, sesgo en los datos, gobernanza de los datos, desarrollo y uso de sistemas de IA. Por lo que, sin un marco general, estos diferentes ciclos de vida de los datos pueden resultar difíciles de interpretar correctamente para quienes no tienen conocimientos, contexto ni experiencia previos. Visto desde otra perspectiva tampoco podemos afirmar que un sistema de IA sea un tratamiento de datos único, pues un mismo tratamiento de datos puede incluir varios sistemas de IA o no formar parte de ningún tratamiento de datos. Por lo que en consonancia con lo que nos plantea la AEPD, consideramos que un sistema de IA se puede encontrar en el marco de cuatro grupos de tratamiento: diseño/desarrollo, distribución (comunicación de datos), operación (pruebas, mantenimiento) y evolución (mantenimiento). A su vez cada uno puede tener distintos responsables del tratamiento en caso de haber tratamiento de datos personales.

Figura 10. Ciclo de vida de una IA y de los datos



Elaboración propia.

Por poner un ejemplo, si se considerase que un organismo público implementara uno o varios sistemas de IA para gestionar el proceso de selección de solicitudes para subvenciones en un futuro, este se llevaría a cabo primero en un entorno de pruebas o Sandbox. Este sistema o sistemas de IA analizaría los datos de los solicitantes para identificar aquellos que cumplen con los requisitos básicos y luego los clasificaría por niveles de prioridad, optimizando así el proceso y reduciendo el tiempo de revisión.

1 Desde la fase de *diseño* está claro que deberá de tenerse en cuenta qué datos se van a tratar para poder entrenar el sistema de IA, igualmente mientras el modelo se *desarrolla* necesitarán datos que se ajusten a unos parámetros para ajustar los algoritmos, documentando cada uno de los procesos. En el Sandbox, cuando hay un tratamiento de datos, se pide cumplimentar el formulario de declaración responsable de *accountability*, donde podremos ver los requisitos en materia de protección de datos, como hoja de ruta y observamos como requerimiento final un informe del DPD.[15]

   Al respecto SEPD 2023, advierte que, la mayoría de los requisitos legales establecidos en la propuesta de Reglamento, aplicarían a los «proveedores» de sistemas de IA. La definición de proveedor en la Propuesta se refiere al desarrollo de un sistema de IA. Sin embargo, el término "desarrollo" o "desarrollar" podría aclararse un poco más.

---

15 *Si se quiere descargar la declaración de responsabilidad, está disponible en:* https://sede.mineco.gob.es/es/Documents/Formulario_declaraci%C3%B3n_responsable.pdf

2. En segundo lugar, en cuanto a lo relativo a la *distribución (despliegue)*, como existe tratamiento de datos es muy probable que exista una comunicación de datos. Tengamos en cuenta que la Administración puede solicitar la colaboración de uno o varios proveedores, operadores, responsables de despliegue; terceros. A todos los que se pedirá que también cumplan en materia de protección de datos y que sus DPD presenten el informe correspondiente.
3. Durante la *operación*, el sistema de IA recibe, procesa y clasifica automáticamente las solicitudes de subvenciones. Analiza los datos personales, como la información económica, antecedentes y otros datos relevantes de los solicitantes, para hacer una preselección en función de los criterios del programa de subvenciones. El sistema debe cumplir estrictamente con el RGPD. En los casos en los que los solicitantes no cumplan con los criterios de IA podrían ser revisados manualmente, asegurando así una evaluación justa y permitiendo que los solicitantes afectados tengan la oportunidad de solicitar una revisión.
4. En la fase de *evolución*, el sistema de IA podría requerir ajustes para optimizar sus algoritmos de selección. Este proceso podría requerir de nuevos datos o la adaptación de los criterios de selección en el modelo. Se debería de realizar una nueva EIPD para poder evaluar los riesgos, si hubiera nuevos tratamientos. Cualquier modificación en el modelo de IA también tendría que notificar a los usuarios finales o interesados, cómo estos cambios podrían afectar la evaluación automatizada de sus solicitudes.Como vemos el enfoque de los tratamientos en torno a cuatro grupos es útil para poder ubicarnos mejor dentro del ciclo de vida de un sistema de IA.

En el ámbito de la IA, el DPD se aprecia quizás como supervisor de la calidad de los datos utilizados para entrenar los algoritmos para que estos no vulneren los derechos de los interesados. Recordemos que, además, se debe de evaluar que siempre exista un supervisor humano detrás de toda IA. Esto apuesta por garantizar que los datos sean precisos, relevantes y estén libres de sesgos, lo que contribuye a la equidad y la no discriminación en los resultados de los sistemas de IA. Ya que son cuestiones que preocupan mucho sobre el futuro de la Inteligencia Artificial. El DPD tendría aquí un papel de refuerzo para el cumplimiento normativo en IA, pero esto podría entrar en situaciones de conflicto de intereses, como hemos visto que nos comunicaba CEDPO, 2024, sobre todo si se toman decisiones respecto de la gobernanza de la IA. Al respecto debemos añadir que los sistemas automatizados procesan el contexto real de la sociedad (Soriano Arnanz, A. 2021) y esto pone en relieve las problemáticas sociales que llevan años muy asentadas en diversos estratos de la sociedad. En los últimos años lo único que ha pasado es que hemos sido testigos de que la IA reproduce las desigualdades sociales tal cual reflejo mismo de lo que está mal implementado, por lo que diversos autores aquí mencionados, indican que de no frenar esto, se estarían perpetuando así las diversas problemáticas y es algo que hay que evitar.

Figura 11. Nuevas funciones generales del DPD en tratamientos de IA

Funciones en tratamientos de IA	Descripción
SUPERVISIÓN DEL USO DE IA EN EL TRATAMIENTO DE DATOS	Asegurar que el cumpla con las normativas de protección de datos, los principios éticos. Asegurar el cumplimiento de leyes y regulaciones específicas que afectan al sector público, como la Ley de Transparencia y Acceso a la Información Pública.
TRANSPARENCIA Y EXPLICABILIDAD	Garantizar que los modelos de IA sean transparentes y explicables, especialmente en procesos administrativos y en la toma de decisiones automatizadas que afecten a los individuos.
MINIMIZACIÓN DE DATOS	Asegurar que los Sistemas de IA. solo utilicen los datos necesarios para su propósito específico y no recojan ni procesen datos innecesarios.
EVALUACIÓN Y GESTIÓN DE RIESGOS, EIPD	Evaluar y gestionar los riesgos asociados con el uso de IA, incluyendo la identificación de posibles impactos en los derechos y libertades de los interesados.
MITIGACIÓN DE SESGOS	Implementar medidas para identificar y mitigar sesgos en los algoritmos de IA que puedan llevar a decisiones discriminatorias o injustas.
AUDITORÍA DE ALGORITMOS	Realizar auditorías periódicas de los algoritmos y modelos de IA para asegurar su conformidad con las normativas de protección de datos y los principios éticos.
SUPERVISIÓN DE PROVEEDORES DE IA	Asegurar que los proveedores de soluciones de IA cumplan con las normativas de protección de datos y los requisitos contractuales, incluyendo la realización de evaluaciones de impacto en la protección de datos cuando sea necesario.
CONSENTIMIENTO INFORMADO	Garantizar que se obtenga el consentimiento informado de los individuos cuando se utilicen datos personales para entrenar modelos de IA, especialmente en contextos donde la toma de decisiones automatizada tenga un impacto significativo.
DERECHOS DE LOS INTERESADOS	Facilitar el ejercicio de los derechos ARSOPOL de los interesados en relación con el tratamiento de datos por sistemas de IA.
RESPONSABILIDAD Y RENDICIÓN DE CUENTAS	Implementar mecanismos para asegurar la responsabilidad y rendición de cuentas en el uso de IA, incluyendo la documentación y justificación de decisiones automatizadas basadas en IA.

Elaboración propia.

En virtud de lo establecido en el Capítulo II del RIA, en lo referente a las prácticas prohibidas de IA, estaría clarísimo que el DPD tiene otro papel de supervisión en refuerzo ya que por un lado velará que se cumpla la normativa y por otro controlará que los sistemas de IA no vulneren los derechos fundamentales de las personas en lo relativo a:

- Sistemas de IA que empleen técnicas subliminales o manipuladoras para distorsionar el comportamiento, afectando la capacidad de tomar decisiones informadas.
- Uso de sistemas de IA que exploten las vulnerabilidades de personas debido a su edad, discapacidad o situación social o económica para distorsionar su comportamiento y causar daño significativo.
- Se prohíbe la comercialización o uso de sistemas de categorización biométrica que clasifiquen a las personas según características como raza, opiniones políticas, afiliación sindical, entre otras, a menos que sea para aplicaciones legales como la aplicación de la ley.
- Puntuación social injusta, evaluar o clasificar personas basadas en su comportamiento social o características personales, si esto conduce a un trato injusto o desfavorable.
- Identificación biométrica en espacios públicos con fines policiales está prohibido, a menos que sea estrictamente necesario para ciertos objetivos como la prevención de delitos graves o terrorismo.
- Evaluaciones de riesgo para delitos, para predecir el riesgo de que una persona cometa un delito basándose únicamente en perfiles o características de personalidad.
- Creación de bases de datos de reconocimiento facial no selectiva, de imágenes faciales de Internet o grabaciones de CCTV.
- Reconocimiento de emociones en entornos laborales y educativos, excepto por razones médicas o de seguridad.

Además, debemos destacar que tanto Comité Europeo de Protección de Datos (CEPD), como el Supervisor Europeo de Protección de Datos (SEPD) se han pronunciado en lo relativo a las prácticas prohibidas.[16]

Pues bien, en materia de riesgos, el reto es amplio para un DPD, vemos como se presenta un alto riesgo (Art. 6 RIA, ANEXO III) en:

- La evaluación de admisibilidad para servicios públicos: los sistemas de IA empleados por autoridades públicas o en su nombre para determinar si una persona física es elegible para recibir servicios y prestaciones

[16] Dictamen conjunto CEPD-SEPD 5/2021 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre inteligencia artificial (Ley de Inteligencia Artificial), 18 de junio de 2021, párrafo 29. Disponible en: https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

esenciales de asistencia pública, incluidos servicios de salud. Engloba la concesión, reducción, retirada o reclamación de devolución de dichos servicios y prestaciones.

- Evaluación de solvencia y calificación crediticia: los sistemas de IA utilizados para evaluar la solvencia o establecer la calificación crediticia de individuos, exceptuando aquellos sistemas diseñados específicamente para detectar fraudes financieros.
- Evaluación de riesgos y precios en seguros de vida y salud: los sistemas de IA utilizados para evaluar riesgos y fijar precios de seguros de vida y salud en relación con personas físicas.
- Gestión de emergencias, triaje: los sistemas de IA destinados a clasificar y priorizar llamadas de emergencia realizadas por individuos, así como para la asignación y establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, como policía, bomberos y servicios médicos de emergencia. Esto engloba sistemas de triaje de pacientes en contextos de asistencia sanitaria de urgencia.

Según establece el articulado del Reglamento de Inteligencia Artificial (RIA), se deben cumplir una serie de obligaciones y requisitos que se pueden resumir de la siguiente manera:

- Transparencia: proveedores e implementadores, independientemente del nivel de riesgo del sistema, deben garantizar que los usuarios finales comprendan cómo y por qué se toman decisiones basadas en IA.
- Formación: proveedores e implementadores, independientemente del nivel de riesgo del sistema, deben asegurarse de que todos reciban formación adecuada sobre el uso seguro y efectivo de los sistemas de IA.
- Vigilancia humana en el uso del sistema: implementadores de sistemas de IA de alto riesgo deben garantizar que siempre haya supervisión humana para intervenir si el sistema de IA actúa de manera imprevista o perjudicial.
- Evaluación de conformidad: proveedores de sistemas de IA de alto riesgo deben llevar a cabo evaluaciones para asegurar que sus sistemas cumplen con las normativas y estándares establecidos.
- Evaluación de Impacto IA: proveedores e implementadores de sistemas de IA de alto riesgo deben realizar evaluaciones para identificar y mitigar posibles riesgos asociados con la implementación y uso de IA.
- Evaluación de Impacto de Protección de Datos: implementadores de sistemas de IA de alto riesgo deben evaluar cómo el uso del sistema afectará la privacidad y protección de datos personales, garantizando el cumplimiento de las normativas de protección de datos.
- Notificación de incidentes: proveedores e implementadores de sistemas de IA de alto riesgo deben notificar de inmediato cualquier incidente relacio-

nado con el uso del sistema que pueda afectar la seguridad o los derechos de las personas.

- Homologación de proveedores: implementadores deben asegurarse de que los proveedores de sistemas de IA cumplan con los estándares y normativas para garantizar la calidad y seguridad del sistema.
- Vigilancia y control: proveedores e implementadores deben establecer mecanismos de vigilancia y control continuo para asegurar que los sistemas de IA operen de manera segura y efectiva a lo largo del tiempo.
- Conservación de registros: proveedores e implementadores deben mantener registros detallados de la operación y uso de los sistemas de IA durante todo el ciclo de vida del sistema, para garantizar la trazabilidad y responsabilidad.

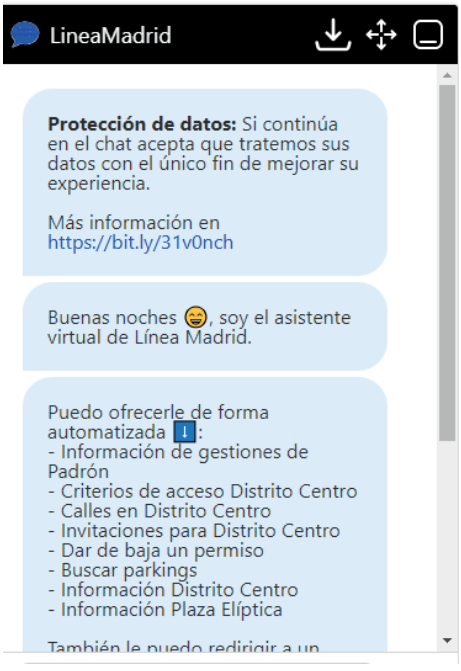
Ahora bien, en el ámbito de las Administraciones Públicas, vemos como en los últimos años han proliferado los asistentes virtuales, que encajan en un riesgo limitado, como ejemplo tenemos Línea Madrid que nada más aparecer en pantalla nos señala un aviso de protección de datos. Que nos dice que si continúanos en el chat aceptamos que tratemos sus datos con el único fin de mejorar su experiencia. Brindándonos un enlace que nos lleva a la segunda capa de información, donde podemos leer la Política de protección de datos. Como a priori, la frase de consentimiento implícito no nos convence visitamos la segunda capa donde buscamos el RAT, encontrando que existen dos bases de legitimación, la primera es el Interés público (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.; Ordenanza ANM 2019/19, de 26 de febrero, de Atención a la Ciudadanía y Administración Electrónica) y la segunda base legitimadora es el consentimiento de la persona afectada. Podríamos atribuir la base de legitimación al interés público, pero también el consentimiento, ya que no se explica con exactitud cuál aplica para *el chatbot*. La idea de este ejercicio es subrayar que apenas se están configurando los asistentes virtuales, puesto que, en las diversas políticas de privacidad, no hay información amplia de lo que pasa con esos tratamientos. Por ejemplo, si le facilitamos datos al *chatbot,* no menciona ¿dónde quedará almacenada la información? por ejemplo, el plazo de conservación si hay comunicación de datos o ¿quiénes tendrán acceso a mis datos? ¿habrá transferencia internacional de datos? por lo que estaremos seguramente a puertas de nuevas guías que nos aclaren estas cuestiones como ya lo hicieron por ejemplo con las cookies. Por su parte se publicaron consejos generales por parte de la AEPD, a través de una infografía[17]. Donde nos orienta a revisar que se ofrezca una política de privacidad con identificación clara del responsable del tratamiento de datos, información para poder ejercer los derechos de protección de datos, así como información sobre si el chatbot continúa aprendiendo de las conversaciones man-

[17] Puede consultarse para ver además los consejos para los usuarios. Disponible en https://www.aepd.es/infografias/info-recomendaciones-chatbots-ia.pdf

tenidas con los usuarios o personas interesadas y qué operaciones realiza con esos datos una vez mejorado. Como apreciamos de momento las Administraciones, se encontrarían en fase de implementación y mejoras de sus políticas de privacidad para completar la información en aras de transparencia RGPD-RIA.

Igualmente, algunos autores como Ponce Solé (2023) no están del todo a favor de *los chatbots*, en su caso argumenta que, si bien los asistentes virtuales pueden ser útiles para brindar información general de manera rápida y directa, no deben tener atribuciones para tomar decisiones. Esto se debe a que, aunque estos servicios de teleasistencia robótica pueden facilitar el acceso a la información, no deben sustituir la atención presencial, ya que ello podría afectar la calidad del servicio público ofrecido a los ciudadanos. De otra perspectiva, es muy común observar las demandas por parte de los ciudadanos más digitales, cuando hablan con un *chatbot* que no facilita una ayuda precisa y que sólo contiene una lista de FAQs, preguntas y respuestas frecuentes, resultando para el ciudadano una pérdida de tiempo más que una ayuda o agilización de la Administración. Es por esta situación que se tendrá que abordar la toma de decisiones conforme a las normativas vigentes llegando a un equilibrio, porque está claro que la Inteligencia Artificial está acelerando sus mejoras y perfilando sus automatizaciones cada año que pasa.

Figura 12. Línea Madrid asistente virtual



Fuente: Madrid.es. Disponible en:
https://www.madrid.es/portales/munimadrid/es/Inicio/Ayuda/Asistente-Virtual-de-Linea-Madrid/

4. CONCLUSIONES

Del contenido de los anteriores epígrafes, podemos determinar que el DPD, se va a configurar en un super guardián de la protección de datos cuando los tratamientos utilicen sistemas de IA. Visto de este modo, se erige en una figura clave para la salvaguardia de los derechos fundamentales de los ciudadanos, asegurando que los datos personales se manejen de manera ética, garantizando el cumplimiento de las normativas de protección de datos, especialmente el RGPD, LOPDGDD, así como el resto de normativa sectorial aplicable para el sector público.

Además, podemos concluir que el DPD se ha ido perfilando y evolucionando a lo largo de estos años, pues casi todos los especialistas estamos acostumbrados a actualizarnos constantemente, convirtiéndose la especialidad en un camino de grandes retos que trae muchas alegrías, así como anécdotas. Ya que está claro que todas las funciones relatadas hay que desarrollarlas con la rigurosidad que se merece pues además de ayudar a los responsables del tratamiento, tenemos una misión más loable que es la de velar que no se vulneren los derechos y libertades de las personas físicas.

Si se diera el caso en los próximos meses que se creara una nueva figura cuyas funciones fueran directas en materia de cumplimiento normativo relativo a IA, igualmente los DPD tendríamos que seguir al pie del cañón, con las funciones anteriormente detalladas. Es nuestro deber el salvaguardar el derecho fundamental a la protección de datos de las personas cuando existan tratamientos de datos personales en el marco de soluciones IA. Nuestro papel seguiría siendo el mismo que tenemos por ejemplo cuando nos relacionamos en el ámbito privado con el Sistema de Gestión de Seguridad de la Información y su figura afín que es el CISO, debiendo trabajar en equipo y alineados a los objetivos en común de cada organización sea pública o privada.

Ahora bien, el sector público parece tomar siempre la delantera porque es quién crea las leyes y también impulsa el uso de la IA, así como la innovación, lo hemos visto con las palancas en las que viene trabajando ENIA, marcado por objetivos que van a dar que hablar a corto plazo y en los próximos años ya que se están considerando grandes partidas presupuestarias para cada uno de los proyectos. La apuesta por cambiar el modelo de Función pública atendiendo al cambio generacional y la apuesta por personal con habilidades digitales sin duda va a cambiar el paradigma de lo que hoy por hoy conocemos en el ámbito de la Administración Pública.

En estos escenarios tan evolutivos el DPD debe estar capacitado para comprender y evaluar los riesgos asociados con el uso de la Inteligencia Artificial en el tratamiento de datos personales. Esto implicaría tener un campo de visión amplio del contexto de los algoritmos utilizados, así como de las implicaciones éticas y conocimiento legal (RIA) de su aplicación en el contexto de la protección de datos. El DPD debe adaptarse continuamente a las innovaciones tecnológi-

cas, asegurando que los sistemas de IA se desarrollen y desplieguen de manera que respeten los principios de protección de datos y minimicen los riesgos asociados. Por ello también se prevé que el DPD tomará un papel importante en el marco de los sistemas de Gestión de IA, pero este escenario plantea dos desafíos importantes; sin que se produzcan conflictos de intereses o que el DPD pierda la independencia que posee.

Igualmente, el DPD debe desempeñar un papel activo en la garantía de la transparencia y la rendición de cuentas en el desarrollo e implementación de sistemas de IA. Esto conlleva la participación en la evaluación de impacto en la protección de datos, específica para proyectos de IA, así como en la comunicación proactiva con las personas físicas sobre cómo se utilizan sus datos y los procesos de toma de decisiones automatizadas.

Dado todo el movimiento que se está generando en torno al uso de la IA, no podemos negar las sensaciones que genera en los ciudadanos, desde el desconocimiento, pasando por el miedo, el rechazo, así como su aceptación sin límites. Ante estas circunstancias los especialistas en esta materia tan apasionante nos convertimos en concienciadores también de la sociedad, donde vemos que hace falta una mayor presencia de divulgadores o concienciadores en materia de privacidad, protección de datos y ciberseguridad. Del resultado de este estudio, podemos corroborar que existen muchas desigualdades sociales y los individuos temen que los algoritmos sigan siendo el fiel reflejo de lo que ya está mal en el ámbito público. Es por ello que las AAPP deberían de escuchar más a los ciudadanos para proponer mejoras realistas, mitigando los sesgos y deteniendo cualquier forma de discriminación.

Dicho lo anterior una de las funciones del DPD que más se va a destacar será la de formación y capacitación en el seno de organizaciones públicas (también en las privadas), pues surge la necesidad de mantener actualizadas las formaciones cuando se den tratamientos de datos personales para de esta forma crear una cultura de privacidad y de protección de datos. La creación de laboratorios de innovación, *sandbox* de IA y la centralización de casos piloto de IA en la AGE facilitan el desarrollo de capacidades y el aprendizaje continuo. El DPD debe estar involucrado en estos procesos para garantizar que las buenas prácticas de protección de datos se integren desde las primeras etapas del desarrollo de los sistemas de IA, promoviendo así en todas las fases del proyecto una cultura de privacidad y seguridad.

Sobre la interacción con el Reglamento de IA, vemos como introduce nuevas obligaciones y desafíos para el DPD, quien debe garantizar que los sistemas de IA cumplan con los estándares de transparencia, ética y mitigación de sesgos. Enfatiza además la necesidad de un enfoque proactivo en la evaluación y gestión de riesgos, particularmente en el uso de datos biométricos y otras formas de datos sensibles.

La implementación de sistemas de IA en el sector público precisa de una estructura de gobernanza centralizada, como la presentada por el proyecto Gov-

Tech de la SGAD. El DPD juega o puede jugar un papel clave en esta estructura, supervisando la conformidad de los sistemas de IA con las normativas de protección de datos y colaborando con diversas entidades públicas para garantizar una implementación coherente y segura. Quizás es pronto para indicar algún presagio, pues apenas estamos en la puesta en marcha y cualquiera de nuestros escenarios puede cambiar, por lo que en los próximos meses nuestro papel debe ser de meros espectadores actualizándonos en las normativas que están por aparecer en el horizonte, como la próxima ley de IA de Galicia, la normativa sobre de simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial.

5. REFERENCIAS

Lista de Referencias

AEPD. (2020). Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. [En línea]. Disponible en https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf [Consulta: febrero de 2024].

AEPD. (2018). El delegado de Protección de Datos en las Administraciones Publicas. [en línea]. Disponible en https://www.aepd.es/documento/funciones-dpd-en-aapp.pdf [Consulta: enero de 2024].

AEPD. (2020). Tecnologías y Protección de Datos en las AA.PP. [En línea]. Disponible en: https://www.aepd.es/guias/guia-tecnologias-admin-digital.pdf [Consulta: febrero de 2024].

AEPD. (2023). Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo. [En línea]. Disponible en https://www.aepd.es/guias/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf>. [Consulta: febrero de 2024].

AEPD. (2023). Gabinete jurídico REF 0059/2023 [En línea]. Disponible en: https://www.aepd.es/documento/2023-0059.pdf [Consulta: octubre de 2024].

AEPD. (2023). Gabinete jurídico REF 0038/2023 [En línea]. Disponible en: https://www.aepd.es/documento/2023-0038.pdf [Consulta: septiembre de 2024].

AEPD. (2023). Protección de Datos y Administración Local. [En línea]. Disponible en: https://www.aepd.es/guias/guia-proteccion-datos-administracion-local.pdf [Consulta: enero de 2024].

Ayuntamiento de Barcelona. (2023) Protocolo "Definición de metodologías de trabajo y protocolos para la implementación de sistemas algorítmicos". INAP.

Berning Prieto, A. D. (2023). El uso de sistemas basados en inteligencia artificial por las Administraciones públicas: estado actual de la cuestión y algunas propuestas ad futurum para un uso responsable. *Revista De Estudios De La Administración Local y Autonómica*, (20), 165–185. https://doi.org/10.24965/reala.11247

Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P.,... & Amodei, D. (2020). Language models are few-shot learners. Advances in neural information processing systems, 33, 1877-1901.

Campbell, M., Hoane, A. J., & Hsu, F. H. (2002). Deep Blue. Artificial Intelligence, 134(1-2), 57-83.

Comisión Europea. (2019). A definition of AI: Main capabilities and scientific disciplines. High-Level Expert Group on Artificial Intelligence. [En línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-12/ai-definition.pdf

Comisión Europea, Centro Común de Investigación (JRC) (2021): Casos seleccionados de IA en el sector público (JRC129301). Comisión Europea, Centro Común de Investigación (JRC) [Conjunto de datos] [En línea]. Disponible en PID: http://data.europa.eu/89h/7342ea15-fd4f-4184-9603-98bd87d8239a

Cotino Hueso, L., Castellanos Claramunt, J. (2022). *Transparencia y explicabilidad de la inteligencia artificial*. Valencia: Tirant Lo Blanch.

Directrices sobre la Evaluación del impacto de protección de datos (EIPD) del GT29 y que establecen si es «probable que el tratamiento resulte en un alto riesgo» a los efectos del Reglamento 2016/679 (GT248, que, en adelante, se denomina Orientaciones sobre las EIPD del GT29) (2017). [En línea]. Disponible en:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

EDPS (2023) Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments. [En línea]. Disponible en: https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2023-10-23-edps-opinion-442023-artificial-intelligence-act-light-legislative-developments_en

FEMP. (2017). TOMO I Guía Para Entidades Locales.[En línea]. Disponible en: https://www.ccn-cert.cni.es/es/pdf/documentos-publicos/ens/2449-femp-ens-tomo-1-guia-estrategica-en-seguridad-para-entidades-locales/file?format=html

Gamero Casado, E. (2023). Inteligencia artificial y sector público. Retos, límites y medios. Tirant Lo Blanch.

Gobierno de España. (2020). Plan de recuperación, transformación y resiliencia. [En línea]. Disponible en: https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/30042021-Plan_Recuperacion_%20Transformacion_%20Resiliencia.pdf

Grupo de trabajo de inteligencia artificial y datos del CEDPO (2024). Is the DPO the right person to be the AI Officer? CEDPO AI and Data Working Group Micro-Insights Series. [En línea]. Disponible en: https://cedpo.eu/wp-content/uploads/The-DPO-and-the-AI-Officer.pdf [Consulta: septiembre de 2024].

Hinton, G. E., Rumelhart, D. E., & Williams, R. J. (1986). Learning representations by back-propagating errors. Nature, 323(6088), 533-536.

INAP. (2023). El Ayuntamiento de Barcelona aprueba un protocolo que garantiza un uso ético de la inteligencia artificial en sus servicios públicos digitales. Disponible en: https://bci.inap.es/alfresco_file/1e08c381-8af2-451a-9102-70f4c061994e [Consulta: mayo de 2024].

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. Advances in neural information processing systems, 25.

Korff, D. Georges M. (2019). El Manual del DPO. Elaborado para el proyecto "T4DATA" financiado por la UE.

McCulloch, W. S., & Pitts, W. 1943. A logical calculus of the ideas immanent in nervous activity. The bulletin of mathematical biophysics, 5(4), 115-133.

Mendoza Balladares, C. P. (2024). Transparencia, Protección de Datos, Open Data y perspectiva del Portal de Datos Abiertos de Canarias. Revista Canaria De Administración Pública, (2), 184–242. https://doi.org/10.36151/RCAP.2.8

Ministerio para la Transformación Digital y de la Función Pública. 2024. Estrategia Nacional de Inteligencia Artificial (2024) [En línea]. Disponible en: https://portal.mineco.gob.es/es-es/digitalizacionIA/Documents/Estrategia_IA_2024.pdf

Ponce Solé, J. (2019). Inteligencia artificial, derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico. Revista General de Derecho Administrativo 50. [En línea]. Disponible en: https://www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=421176

Rodríguez Ayuso, J.F. (2021). La figura del Data Protection Officer en la contratación Pública. Revista digital de Derecho Administrativo. Número 25 pp 309-336

Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach. 4th Edition.

Saíz Peña, C.A. y Balanzategui Vidal B. (2019). El libro blanco del DPO. ISMS Forum. Data Privacy Institute.

Sanz Marco. L. Marzo, A. Moro Cordero M.A. (2023). La autoevaluación en materia de protección de datos: un ejercicio de responsabilidad proactiva de las entidades locales.

Sentencia del Tribunal de Justicia de la Unión Europea de 9 de febrero de 2023, asunto C-453/21 Caso X-FAB Dresden GmbH & Co. KG contra FC. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX%3A62021CJ0453 [Consulta: mayo de 2024].

Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., Van Den Driessche, G.,... & Hassabis, D. 2016. Mastering the game of Go with deep neural networks and tree search. Nature, 529(7587), 484-489.

Soriano Arnanz, A. (2021). Decisiones automatizadas. Problemas y soluciones jurídicas: más allá de la protección de datos. Revista de Derecho Público: Teoría y Método, 3, 85-127. https://doi.org/10.37417/RPD/vol_3_2021_535

Tangi, L., Combetto, M., Martin Bosch, J. y Rodríguez Müller, P., Inteligencia artificial para la interoperabilidad en el sector público europeo, Oficina de Publicaciones de la Unión Europea, Luxemburgo, (2023), doi:10.2760/633646, JRC134713.

Tecnologías de la información – Inteligencia artificial – Marco del ciclo de vida de los datos (ISO/IEC 8183:2023) (Ratificada por la Asociación Española de Normalización en julio de 2024.)

Tecnología de la información – Inteligencia artificial – Sistema de gestión (ISO/IEC 42001:2023).

Turing, A. M. (1950). Computing Machinery and Intelligence. Mind, 59(236), 433-460.