https://doi.org/10.18800/iusetveritas.202502.004

El rol del delegado de protección de datos en Europa tras la aprobación del Reglamento UE de Inteligencia Artificial(*)

The role of the data protection officer in Europe following the approval of the EU regulation on Artificial Intelligence

Rubén Martínez Gutiérrez(**)
Universidad de Alicante (San Vicente del Raspeig, España)

Resumen: Las personas Delegadas de Protección de Datos en la Unión Europea se encuentran en un momento de cambio creciente en cuanto a su estatuto jurídico y funciones, derivado de las nuevas normas en materia de datos, interoperabilidad e Inteligencia Artificial. Estos cambios afectan de forma especial al sector público, lo que será analizado específicamente en este trabajo. En este artículo se analizan las funciones esenciales de las personas DPDs derivadas de la normativa de protección de datos, y también aquellas que se prevén adicionar como consecuencia del nuevo marco normativo de la UE, con especial interés en la supervisión de *sandboxes* y en las evaluaciones de impacto en materia de derechos fundamentales en Inteligencia Artificial.

Palabras clave: Delegado de Protección de Datos - Rol - Funciones - Datos - Interoperabilidad - Inteligencia Artificial - Derecho Administrativo - España

Abstract: Data Protection Officers in the European Union are undergoing a period of increasing change in terms of their legal status and functions, as a result of new regulations on data, interoperability and Artificial Intelligence. These changes particularly affect the public sector, which will be analysed specifically in this paper. This article analyses the essential functions of DPOs derived from data protection regulations, as well as those that are expected to be added as a result of the new EU regulatory framework, with a particular focus on the supervision of sandboxes and impact assessments on fundamental rights in artificial intelligence.

Keywords: Data Protection Officer - Role - Functions - Data - Interoperability - Artificial Intelligence - Administrative Law - Spain

(*) Nota del Equipo Editorial: Este artículo fue recibido el 15 de agosto de 2025 y su publicación fue aprobada el 05 de diciembre de 2025.

(**) Abogado por la Universidad de Alicante (San Vicente del Raspeig, España). Doctor Europeo por la Universidad de Alicante. Delegado de Protección de Datos y Catedrático de Derecho de Administrativo de la Universidad de Alicante. ORCID: https://orcid.org/0000-0001-6667-1120. Correo electrónico: ruben.martinez@ua.es.

1. Introducción

La legislación europea y de los Estados Miembros en materia estricta de protección de datos es una legislación ya consolidada. Como es bien sabido, en la Unión Europea contamos con el Reglamento (UE) 2016/679 - Reglamento general de protección de datos (en adelante, RGPD). El Parlamento Europeo y del Consejo, emitido el 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). La RGPD es una norma que ya tiene 10 años y que ha supuesto una variación importante respecto al establecimiento en el plano de igualdad al consentimiento de otras bases de licitud del tratamiento en el artículo 6 de la norma.

Al tratarse de un Reglamento (UE), el artículo 99 señala que la RGPD "será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro". De manera que, a diferencia de lo que sucedió con la Directiva anterior, derogada por esta norma, nos encontramos con un marco normativo más uniforme y directamente aplicable en todos los Estados Miembros. Además, en España, contamos con una Ley de desarrollo del Reglamento UE, la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), que tal y como reconoce en su artículo 1 tiene como objeto "adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679", por lo que la Ley Orgánica española viene a complementar y desarrollar la norma europea.

En este contexto normativo, las y los Delegados de Protección de Datos tenemos una serie de funciones, obligaciones y responsabilidades determinadas que ya venimos desarrollando desde la entrada en vigor del RGPD. Pero en los últimos cinco años, la situación normativa en materia de datos, interoperabilidad e Inteligencia Artificial ha cambiado considerablemente, estableciéndose un nuevo marco normativo en Europa que nos permite hablar de la existencia de una auténtica "Reforma para una Administración de Datos" (Martínez, 2023), en la que las y los Delegados de Protección de Datos parece que vamos a tener que asumir un renovado protagonismo no solo en materia estricta de protección de datos, sino también en ámbitos como la gobernanza de datos y los Espacios de Datos, los entornos de pruebas y/o *sandboxes*, especialmente en materia de interoperabilidad de datos, o la evaluación, o incluso quizá también supervisión interna de los sistemas de Inteligencia Artificial. Esto último principalmente cuando se trate de sistemas de alto riesgo que exijan la realización de evaluación de impacto en materia de derechos fundamentales. Este nuevo marco normativo en la UE se divide en tres bloques: datos, interoperabilidad e inteligencia artificial, los cuales están formado por las siguientes normas:

a) Datos:
- La Directiva 1024/2019, del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público.
- Reglamento (UE) 2022/868, relativo a la gobernanza europea de datos (Reglamento de Gobernanza de Datos).
- Reglamento de Ejecución 2023/138 de la Comisión, que aprueba la lista de conjuntos de datos específicos de alto valor y modalidades de publicación y reutilización.
- Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos).
- Toda la normativa relativa a los Espacios de Datos y especialmente la norma que ya está aprobada relativa al Espacio de Datos de Salud como el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero de 2025, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847.

b) Interoperabilidad:
- Reglamento (UE) 2024/903 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, por el que se establecen medidas a fin de garantizar un alto nivel de interoperabilidad del sector público en toda la Unión (Reglamento sobre la Europa Interoperable).

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

En el presente artículo, intentaremos arrojar a la luz la nueva situación del rol de las y los Delegados de Protección de Datos en Europa que se vislumbra a partir del primer cuarto del Siglo XXI, con el objetivo de servir de marco de referencia para lo que pueda ser extrapolable al régimen y estatuto jurídico de los DPDs en Perú en el futuro.

2. Funciones mínimas del Delegado de Protección de Datos (DPD) en el RGPD de la Unión Europea (UE)

Según el artículo 39 del RGPD de la UE, la persona que ostente la Delegación de Protección de Datos tendrá como mínimo las siguientes funciones:

- Primero, "a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben". En este sentido, la labor de elaboración de dictámenes e informes jurídicos, aparte de resultar una función mínima obligatoria, es absolutamente esencial para garantizar la adecuación de los tratamientos a la normativa de protección de datos.
- Segundo, "b) Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes". Aquí se trata de una función de enorme relevancia y muchas veces olvidada, especialmente en cuanto a la formación se refiere, y que resulta clave para el cumplimiento adecuado del marco normativo.
- Tercero, "c) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación". Esta función de asesoramiento en cuanto a la evaluación de impacto y su control posterior es básica para garantizar el cumplimiento del artículo 35 del RGPD, que sin duda es de gran relevancia en el ámbito de la UE, razón por la cual vamos a dedicar el siguiente apartado.
- Cuarto, "d) Cooperar con la autoridad de control". Se trata de una función sin duda relevante y que puede ser muy beneficiosa para la organización en la que presta sus servicios la persona que ostente la Delegación de Protección de Datos. En el caso de España, como es bien sabido, la autoridad de control es la Agencia Española de Protección de Datos (AEPD). Por ello, la cooperación puede resultar de enorme ayuda para comprender las razones, identificar posibles fallos y determinar futuras soluciones ante incidentes, de manera que la actividad de supervisión se realice de forma satisfactoria para los intereses de la propia organización. Esta se verá beneficiada no solo en cuanto a un mejor funcionamiento en materia de protección de datos, sino también respecto de la percepción que la propia autoridad de control tenga sobre lo sucedido, lo que podría mitigar el impacto de la responsabilidad.
- Por último, "e) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto". Esta constituye otra de las funciones de gran importancia en la actividad de los DPDs, ya que ayuda a que la interlocución entre el responsable del tratamiento y la autoridad de control se produzca de una forma más precisa. Ello ocurre al realizarse por la persona que ostente la Delegación de Protección de Datos, quien, gracias a su cualificación técnica, realizará la consulta que corresponda de una manera más adecuada y ajustada a las necesidades de la organización, con el fin de solventar las dudas que puedan surgir.

Finalmente, y aunque no aparezca expresamente entre las funciones mínimas establecidas en el RGPD de la UE, también resulta interesante destacar la función que el artículo 37 de la LOPGDD española le atribuye, en relación a la "intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos". Con carácter previo al ejercicio de acciones ante las autoridades de control y supervisión, las personas que hayan visto vulnerados sus derechos o quieran realizar una solicitud de ejercicio de los mismos, suelen dirigirse al Delegado de Protección de Datos para que solucione la cuestión. Tal como señala la ley española en el artículo 37, "en este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación". Por esta razón, se habilita un procedimiento previo que puede conllevar a que la persona afectada no inicie el procedimiento de reclamación ante la AEPD.

Tanto es así, que el apartado 2 de dicho artículo señala que "cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos", sin haberse dirigido previamente al DPD de la organización, las autoridades de control "podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes", dando la oportunidad a que el procedimiento de reclamación termine de esta manera. Ahora bien, la Ley también advierte que "si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento"; por lo tanto, ya con una intervención de la autoridad de control en el sentido y dirección que corresponda.

3. La evaluación de impacto en la Protección de Datos

La normativa UE de protección de datos de 2016 reforzó los mecanismos de evaluación ante tratamientos de datos de carácter personal, especialmente cuando se pudiera poner en riesgo los derechos y libertades de las personas respecto de las cuales se está produciendo un tratamiento de datos de carácter personal. En esta línea, el artículo 35 del RGPD estableció un mecanismo de control y supervisión previo a los tratamientos que, por su importancia y utilidad, ha trascendido a día de hoy la protección de datos para extenderse a otros ámbitos como la Inteligencia Artificial, como veremos más adelante.

En esta labor de evaluación y supervisión previa de los tratamientos emerge con fuerza la figura de la persona que ostente la Delegación de Protección de Datos, también del responsable de seguridad informática de la organización, como garante de que estos instrumentos se han aplicado y realizado adecuadamente, así como también para determinar en qué supuestos se debe exigir su realización. Además, el propio RGPD señala en el apartado 2 del artículo 35 que "el responsable del tratamiento recabará el asesoramiento de la persona que ostente la Delegación de Protección de Datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos", con lo que la colaboración y participación de los DPDs en el correcto funcionamiento de estos mecanismos de evaluación es parte esencial de sus funciones.

En esta línea y como ya hemos comprobado, el instrumento denominado "evaluación de impacto relativa a la protección de datos" que regula el artículo 35 del RGPD tiene una especial relevancia. Por un lado, el apartado 1 de este artículo, el cual determina que "una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares", antes señala lo siguiente:

> Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales (RGPD, 2016).

Por otro lado, el apartado 3 establece cuándo será preceptiva la realización de la evaluación de impacto, aunque lógicamente no impide que la misma se realice fuera de estos supuestos si así lo considerase necesario el DPD o el responsable del tratamiento. Este precepto señala que se requiere evaluación de impacto en los siguientes tres bloques de tratamientos:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, u
c) observación sistemática a gran escala de una zona de acceso público (RGPD, 2016).

Una buena práctica en este sentido puede ser requerir la realización de evaluación de impacto cuando se vayan a realizar tratamientos de categorías especiales de datos, particularmente las establecidas en el artículo 9.1 del RGPD. Bajo este apartado, queda prohibida la materia que se refiera a tratamientos de datos personales que puedan revelar lo siguiente:

> El origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física (RGPD, 2016).

Asimismo, en el apartado 4 de este artículo se indica que "la autoridad de control",

que en el caso de España es la Agencia Española de Protección de Datos, "establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos", cuestión que se ha producido en España y que se encuentra debidamente disponible en la web de la AEPD(1). La otra cara de la moneda se establece en el apartado 5, ya que en el mismo se señala que "la autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos", que también se encuentra publicada en la web de la AEPD(2). No obstante, respecto a la adopción de ambas listas por la autoridad de control a la que se refieren dichos apartados, el apartado 6 del artículo 35 del RGPD, señala que la autoridad de control competente necesariamente debe implicar que se aplique con anterioridad lo siguiente:

> El mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión (RGPD, 2016).

En cuanto al contenido de las evaluaciones de impacto, es decir, aquello que debe conllevar la evaluación, el apartado 7 del artículo 35 establece que la evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas (RGPD, 2016).

En cuanto a las fórmulas de desarrollar la evaluación de impacto y los posibles sistemas a utilizar, interesa destacar que la AEPD dispone de la herramienta Gestiona RGPD para el asesoramiento y realización de evaluaciones(3), aunque se trata de un instrumento esencialmente pensado para el ámbito o sector privado. En el ámbito público, también destacan algunas iniciativas de mecanismos o formularios de evaluación de impacto; por ejemplo, el desarrollado por la Delegación de Protección de Datos de la Universidad de Alicante(4).

Finalmente, como mecanismo de prevención y garantía que es, la evaluación de impacto puede sustentarse en los "códigos de conducta de la entidad", de acuerdo con el apartado 8. Además, según el apartado 9, cuando resulte pertinente, el responsable del tratamiento podrá recabar "la opinión de los interesados o de sus representantes en relación con el tratamiento previsto", para disponer de una información más precisa sobre el tratamiento sometido a evaluación de impacto. Por otro lado, los apartados 10 y 11 se refieren para terminar a evaluaciones de impacto en tratamientos más globales, donde se deberá examinar si la misma cumple específicamente los requerimientos del tratamiento concreto que deba someterse a evaluación de impacto en materia de protección de datos, cuestión que será especialmente necesaria cuando exista un cambio o variación del riesgo en las operaciones de tratamiento.

4. La posición del Delegado de Protección de Datos

Una de las cuestiones más importantes a tener en cuenta en el rol o estatuto de la persona que ostente la Delegación de Protección de Datos es su posición en relación con otras figuras, como el responsable del tratamiento o el encargado.

(1) Para mayor información, *véase* las "Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4)", publicado en la página web de la Agencia Española de Protección de Datos (2019a). Recuperado el 29 de julio de 2025. https://www.aepd.es/documento/listas-dpia-es-35-4.pdf.

(2) Para mayor revisión sobre las listas de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos, *véase* la página web de la Agencia Española de Protección de Datos, en la cual se publicó un documento recopilando dichas listas (2019b). https://www.aepd.es/documento/listasdpia-35.5l.pdf.

(3) Si precisa más detalles sobre dicha herramienta, *véase "*Gestiona RGPD" en la página web de la Agencia Española de Protección de Datos. https://www.aepd.es/guias-y-herramientas/herramientas/gestiona2.

(4) Para una mejor visualización del desarrollo de dicha herramienta, *véase* la sección Documentación y descargue el "Formulario de Evaluación de Impacto" del sitio web oficial de la Universidad de Alicante. https://dpd.ua.es/

Se trata de órganos diferenciados con funciones diferentes, tal y como se puede comprobar en la Figura 1, que, aunque específicamente referido a las brechas de datos, nos da una idea de los diferentes roles y funciones.

Figura 1

Funciones y responsabilidades de las figuras implicadas en la brecha de datos personales

Figura	Funciones y responsabilidades
Responsable	• Implantación del proceso de gestión de brechas • Evaluación de las consecuencias para los derechos y libertades de las personas • Notificar la brecha de datos personales a la Autoridad de Control • Comunicar la brecha de datos personales a las personas afectadas
Encargado	• Informar al responsable de las brechas de datos personales que afecten a los tratamientos encargados • Ayudar al responsable en la gestión de la brecha de datos personales • Ejecutar las labores de notificación o comunicación de la brecha que tenga asignadas por contrato
Delegado de protección de datos	• Informar y asesorar al responsable/encargado del tratamiento sobre sus obligaciones y responsabilidades con relación a las brechas de datos personales • Cooperar con la Autoridad de Control en las cuestiones relativas a la gestión de la brecha de datos personales • Actuar como punto de contacto con la Autoridad de Control, en particular, en el proceso de notificación de la brecha de datos personales

Nota. De "Guía para la notificación de brechas de datos personales", por Agencia Española de Protección de Datos, 2021.

Respecto a la posición en concreto del DPD, se refieren los artículos 38 del RGPD de la UE y 36 de la Ley española de protección de datos (LOPDGDD). La idea esencial de la regulación es otorgar al DPD de independencia en el ejercicio de sus funciones (Sanz, 2018, p. 681), ya que la legislación viene a determinar que el responsable y el encargado del tratamiento garantizarán que la persona que ostente la Delegación de Protección de Datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. Asimismo, bajo el apartado 3 del artículo 38 del RGPD, se determina que "no será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones" y que "rendirá cuentas directamente al más alto nivel jerárquico" de la organización.

Para asegurar esa posición de independencia y de asesoramiento técnico especializado, la normativa, según el apartado 2 del artículo 38, determina que se garantice que el DPD disponga de "los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados". Tan relevante es esa posición neutral, que al final del artículo 38 se señala que, aunque el "delegado de protección de datos podrá desempeñar otras funciones y cometidos", dichas funciones y cometidos no deben dar lugar a conflicto de intereses, es decir, una labor que pueda suponer una merma en el ejercicio imparcial de sus funciones.

La LOPDGDD española es todavía más incisiva en la necesidad de independencia del DPD, ya que establece en su artículo 36.2 que "el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio". Por lo tanto, este artículo deja claro que "se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses". De acuerdo con el artículo 36.4 de la LOPDGDD, el objetivo de garantizar esa posición de independencia es asegurar que "cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento", sin que esté condicionado a actuar de manera diferente por presiones de ningún tipo.

5. Actividades importantes del DPD en el sector público y/o universidades

Particularmente en el sector público, las y los Delegados de Protección de Datos están comenzando a asumir un papel crucial en el funcionamiento de las organizaciones, cuestión que resulta de especial trascendencia en el sector público y en particular en las Universidades (Sanz, 2018, pp. 676-677). En este punto, a título ejemplificativo, me gustaría poner de manifiesto las actividades

que venimos desarrollando desde la Delegación de Protección de Datos de la Universidad de Alicante.

En primer lugar, una de las tareas trascendentales es la relativa a informar y asesorar. Desde que tomé posesión como Delegado de Protección de Datos en 2022, se han realizado un total de 50 informes que se han publicado como Doctrina del DPD de la Universidad de Alicante(5), y que, sin duda, han servido para fomentar una cultura y conocimiento de la protección de datos y sus implicaciones en toda la organización. En esta misma línea, también se encuentra la función de dictar circulares, instrucciones, etc., conjuntas o de la propia Delegación sobre actividades que conllevan tratamientos de datos de carácter personal; por ejemplo, la Instrucción conjunta de la Defensoría Universitaria, la Delegación de Protección de Datos, el Vicerrectorado de Ordenación Académica y Profesorado, el Vicerrectorado de Estudiantes y Empleo y el Vicerrectorado de Igualdad, Inclusión y Responsabilidad Social sobre la utilización de grupos de aplicaciones de mensajería instantánea, como espacio virtual universitario(6), así como otras en cuestiones diversas.

Esta labor ha sido esencial para cumplir con la segunda actividad básica que es supervisar el cumplimiento del RGPD y de la LOPDGDD, así como realizar un control interno de la organización en materia de protección de datos. Muchos órganos de la Universidad ya conocen la posición de la Delegación de Protección de Datos al encontrarse disponible en abierto nuestra Doctrina y ello facilita en buena medida la labor de supervisión y control, especialmente desde la perspectiva de la prevención.

En tercer lugar, y como ya hemos analizado en el apartado 3 de este trabajo, el DPD también debe supervisar "las evaluaciones de impacto", siendo una de las funciones esenciales a día de hoy.

Asimismo, en cuarto lugar, está la importante función de cooperar con la autoridad de control. En nuestro caso, lo realizamos en conjunto con la AEPD, en cuestiones importantes de seguridad y protección de datos, como la gestión de brechas de seguridad o en los procedimientos sancionadores, siendo estas unas funciones que pueden mitigar los efectos de una posible sanción si ha existido una colaboración adecuada.

En quinto lugar, una función esencial y cada vez más trascendental del DPD en el sector público y, en particular, en las universidades, es su participación en Comisiones y Comités; por ejemplo, el Comité de Ética de la Investigación, Comité de Seguridad de las Tecnologías de la Información, Comisión de Administración Digital y Simplificación, etc. Se trata de una participación clave en muchas de ellas. Especialmente, en el caso de los Comités de Ética de la Investigación, ya que se trata de una obligación legal determinada en la Disposición Adicional Decimoséptima de la LOPDGDD, que expresamente determina lo siguiente:

> En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados (UE, 2018).

En sexto lugar, otra de las actividades básicas de los DPDs en el sector público es la de velar por el cumplimiento de las obligaciones y garantizar los derechos de acceso, rectificación, cancelación, oposición, limitación, supresión, olvido, etc. Esto mediante la función de asesoramiento y propuesta de resolución al responsable del tratamiento ante peticiones y solicitudes a estos efectos. En este punto, también es importante destacar la propuesta de informe sobre las cesiones de datos que se soliciten, y que finalmente debe autorizar el responsable del tratamiento.

En séptimo lugar, el DPD también debe supervisar el Registro de Actividades de Tratamiento regulado en el artículo 31 de la LOPDGDD. Si bien es una obligación de los responsables y encargados del tratamiento, el Delegado debe participar activamente, ya que la propia regulación en el artículo 31 establece que "cuando el responsable o el encargado

(5) Para observar dichos informes, *véase* "Doctrina de la Delegación de Protección de Datos", publicada en la página oficial de la Delegación de Protección de Datos. https://dpd.ua.es/es/doctrina-de-la-delegacion-de-proteccion-de-datos.html

(6) Para una mayor revisión, *véase* "Instrucción conjunta de la defensoría universitaria, la delegación de Protección de Datos, el vicerrectorado de Ordenación Académica y Profesorado, el vicerrectorado de Estudiantes y Empleo y el vicerrectorado de Igualdad, Inclusión y Responsabilidad social sobre la utilización de grupos de aplicaciones de mensajería instantánea como espacio virtual universitario", publicado por la Universidad de Alicante. https://web.ua.es/es/vr-oacademica/normativa-y-procedimientos/instruccion-def-universitario-dpd-voap-vee-viirs.pdf

del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro", siendo por tanto una labor de supervisión necesaria y, además, preceptiva, según la legislación.

Finalmente, en octavo lugar, es importante destacar otras funciones vinculadas a la formación, como la realización de cursos, congresos, seminarios, etc. Se trata de una tarea de enorme relevancia en la práctica, pues tiene un impacto muy positivo en el buen funcionamiento de la organización en materia de protección de datos. Sin duda, sería importante dedicar más recursos económicos a este tipo de actividades, ya que son clave en materia de prevención y buenas prácticas, consiguiendo un funcionamiento de la organización mucho más ajustado a la normativa de protección de datos.

6. Nuevas funciones en el horizonte: Datos, interoperabilidad e Inteligencia Artificial

Tal y como anunciamos en la introducción de este trabajo de investigación, en la Unión Europea se ha configurado en los últimos años un nuevo marco normativo que afectará decididamente al rol y funciones de los Delegados de Protección de Datos. Este nuevo marco normativo se divide en tres bloques: (i) datos, (ii) interoperabilidad y (iii) la Inteligencia Artificial[(7)], y del mismo se desprenden una serie de derechos, obligaciones y previsiones que pueden tener afectación en las funciones que desarrollen los DPDs. Por ello, en cuanto a las nuevas normas en materia de datos, los Delegados de Protección de Datos deberán asumir nuevas funciones en cuatro ámbitos:

- Las interrelaciones entre la normativa de transparencia y de protección de datos en el sector público, con especial interés en la ponderación del derecho de acceso a la información y su conflicto con la normativa de protección de datos, decidiendo sobre cuestiones como la anonimización de documentos y expedientes, la posibilidad del acceso parcial a los mismos y el diseño de los archivos de las Administraciones y organismos públicos, basados en el principio de privacidad desde el diseño que permita un ejercicio más adecuado de la transparencia con total garantía de la normativa de protección de datos.
- La reutilización de datos en el sector público, pues cada vez nos encontramos con más frecuencia ante solicitudes de reutilización de información, datos y documentos del sector público. Ante las mismas, los responsables del tratamiento requieren el asesoramiento e informe de la persona que ostente la Delegación de Protección de Datos para asegurar que la aceptación de la solicitud se adecúa tanto a la normativa de reutilización, como a la de protección de datos.
- La calidad de los datos, en el sentido de supervisar el proceso de archivo y almacenamiento en condiciones óptimas para poder compartir los datos de forma interoperable y sin vulnerar la normativa de protección de datos, configurando adecuadamente los sistemas de almacenamiento de datos en base a los principios de privacidad desde el diseño.
- El diseño de los Espacios de Datos, ya que las nuevas obligaciones y posibilidades en materia de Espacios de Datos que afectan a las organizaciones del sector público están determinando que los Delegados de Protección de Datos deban asumir funciones de control y supervisión de los procesos, en los cuales la interoperabilidad también será un actor clave.

Con respecto a la nueva regulación UE de interoperabilidad, que también incluye parte de las funciones que acabamos de ver en el párrafo anterior, especialmente en cuanto a la calidad de los datos y al diseño de los Espacios de Datos, parece que la normativa establece nuevas obligaciones de supervisión de los *sandboxes* o entornos de pruebas en materia de interoperabilidad, que implican un conocimiento profundo de la nueva normativa y de sus requerimientos. Se podría afirmar así que, de alguna manera, los Delegados de Protección de Datos van a tener que liderar en el sector público la denominada "Administración de Datos", que Martínez la define como:

> Aquella en la que los datos se sitúan en el centro del obrar administrativo, para lo cual será necesario diseñar adecuadamente el archivo único de cada Administración pública basándose en una gestión documental plenamente interoperable que permita conseguir una mejor garantía en los derechos de las personas gracias a técnicas avanzadas y automatizadas que tengan como eje al dato, tales como el acceso al dato mínimo necesario para la tramitación de los procedimientos administrativos (2023, p. 70).

(7) Respecto a la referencia concreta de las normas nos remitimos al apartado 1 de este trabajo.

Un ejemplo de determinación de nuevas funciones a los DPDs en esta materia es la Ley 2/2025 de Galicia (España) para el desarrollo e impulso de la Inteligencia Artificial. Pues, esta ley en su artículo 49 establece que, relativo a los *sandboxes*, "en la medida en que los sistemas de inteligencia artificial impliquen el tratamiento de datos personales, la autoridad competente en materia de protección de datos esté vinculada al funcionamiento del espacio controlado de pruebas". Esto deja clara la participación de los DPDs en este ámbito. Por tanto, y en cuanto a este bloque de nuevas funciones, nos parece especialmente interesante y trascendente la de supervisión del funcionamiento y puesta en marcha de los *sandboxes*, razón por la cual realizaremos su estudio detallado en el apartado 7 del presente artículo.

Para finalizar, la nueva normativa UE de Inteligencia Artificial también determina una serie de nuevas obligaciones que van a implicar la asunción de nuevos roles a los Delegados de Protección de Datos, particularmente a aquellos que ejercen sus tareas en el sector público. No en vano, muchas de las entidades y asociaciones, tradicionalmente dedicadas a la privacidad y a la protección de datos, se están arrogando también nuevas funciones en el ámbito de especialización de la Inteligencia Artificial, por la importancia que la gestión de los datos tiene en estas tecnologías. Un ejemplo claro es la Asociación Profesional Española de la Privacidad (APEP), que en breve añadirá a su denominación "y de la Inteligencia Artificial". De alguna forma, es un camino natural por diversas razones y cuestiones reguladas en el Reglamento UE de Inteligencia Artificial:

a) Por la importación al ámbito de la IA de la evaluación de impacto, ahora más general y de derechos fundamentales, como instrumento clásico de la protección de datos y en el que, como hemos visto en el apartado 3 de este trabajo, los Delegados de Protección de Datos tienen gran experiencia en su realización y supervisión. Esta realidad implica que, de forma casi natural, los DPDs sean los órganos con mayores conocimientos técnicos para desarrollar también esta tarea fundamental, cuya importancia para el desarrollo de la IA es clave, razón por la cual nos detendremos en su análisis en el siguiente apartado de este artículo.
b) El Reglamento UE de IA ha establecido que la potestad sancionadora en materia de IA para las instituciones comunitarias de la UE recaiga en el *European Data Protection Supervisor* (EDPS), que es la autoridad de control en materia de protección de datos de la UE. La nueva norma UE de IA, a diferencia de otras normas como, por ejemplo, el RGPD, ha decidido establecer un sistema sancionador en el que las AAPP pueden ser objeto de sanciones pecuniarias, cuestión que no era habitual hasta el momento. Sin ánimo de ser exhaustivos en esta cuestión, el Reglamento UE de IA ha determinado en su artículo 100 la potestad de imposición de multas administrativas a instituciones, órganos y organismos de la Unión, como ya hemos advertido a cargo de Supervisor Europeo de Protección de Datos, con importes pecuniarios considerables, aunque si bien es cierto, mucho menores que para los sujetos privados, en base a los cuales se podría llegar a imponer sanciones de hasta 1,5 millones de euros.
c) Evaluación de proyectos de IA con garantía de cumplimiento del RGPD (y en breve también del Reglamento UE de IA). En el caso de los DPDs del sector público, que como hemos señalado ya tienen funciones relevantes y preceptivas por Ley en materia de Comités de Ética de la Investigación, muchas convocatorias públicas de subvenciones dirigidas al desarrollo e implantación de sistemas de IA están exigiendo como requisito previo de admisión de los proyectos que se emita una memoria o documento avalado por el responsable del tratamiento de datos y/o la persona que ostente la Delegación de Protección de Datos que determine que el proyecto cumplirá con la normativa de protección de datos y particularmente con el RGPD. Este tipo de documentos se ampliarán en breve también al cumplimiento de las obligaciones de la normativa de IA, y en este sentido, los DPDs volverán a ser los órganos que técnicamente tienen unas competencias previas más adecuadas para realizar estas funciones.
d) En el caso de organizaciones privadas y en algún caso del sector público, los DPDs también deberán observar que se cumplen con los requisitos de la legislación relativos al cumplimiento de las obligaciones de mercado en materia de IA, cuestión que de alguna manera está latente en el anteproyecto de Ley de IA de España.

En este punto, también hay que destacar algunos ejemplos prácticos de cómo la normativa va a afectar a la asunción de nuevas funciones por los Delegados de Protección de Datos. Además, volviendo a la Ley 2/2025 de Galicia, promulgada para el desarrollo e impulso de la Inteligencia Artificial, la misma determina con claridad en su "Disposición Adicional Única" un precepto

sobre la "atribución de funciones de las personas comisionadas de inteligencia artificial". A partir de este precepto, "las funciones de las personas comisionadas en la Administración general de la Comunidad Autónoma de Galicia y su sector público serán desempeñadas por las personas delegadas de protección de datos". Interesa destacar que las funciones de las personas comisionadas de Inteligencia artificial que en Galicia tienen que desarrollar por imperativo legal los DPDs se vinculan a garantizar el "cumplimiento de los principios y obligaciones en materia de prevención, detección y eliminación de riesgos y de resultados negativos de la implementación de los sistemas de inteligencia artificial diseñados o empleados por la Administración", según el apartado 1 del artículo 36. Además, el apartado 3 de dicho artículo, especifica y detalla las siguientes garantías:

a) Velar por un uso ético y responsable de la inteligencia artificial (Presidencia de la Xunta de Galicia, 2025).
b) Supervisar el diseño, desarrollo, implementación y uso de los sistemas de inteligencia artificial (Presidencia de la Xunta de Galicia, 2025).
c) Asesorar y advertir sobre los riesgos presentes y futuros del diseño, desarrollo y uso de los sistemas de inteligencia artificial (Presidencia de la Xunta de Galicia, 2025).
d) Recibir las sugerencias y quejas de irregularidades en el diseño, desarrollo, implementación y uso de los sistemas de inteligencia artificial (Presidencia de la Xunta de Galicia, 2025).

Para terminar, interesa realizar una importante reflexión, aunque sea breve, respecto a toda esta situación. Con carácter general, la figura de la persona que ostente la Delegación de Protección de Datos se ha caracterizado por tener un carácter o perfil jurídico, dado que así se desprende de las obligaciones y funciones que determina la normativa. Si finalmente como todo parece apuntar, el nuevo marco normativo implica todas o parte de las nuevas funciones que hemos señalado en este apartado, será necesario reforzar las Delegaciones de Protección de Datos también con perfiles de ingeniería o técnicos, para poder desarrollar con garantías las labores de informe, asesoramiento, supervisión y control también en materia de datos, interoperabilidad e Inteligencia Artificial. La combinación de perfiles jurídicos y técnicos sí permitirá el adecuado ejercicio de estas nuevas funciones, pero difícilmente se podrá acometer con garantías estas nuevas obligaciones solo con una formación jurídica, ya que, por muy sólida que sea, se antoja insuficiente[8].

7. En especial, la evaluación del impacto de la IA en materia de derechos fundamentales

Como ya hemos advertido, una de las funciones y actividades en las que se prevé que los Delegados de Protección de Datos puedan asumir protagonismo en el futuro es la evaluación de impacto en materia de derechos fundamentales en Inteligencia Artificial.

El Reglamento UE de Inteligencia Artificial establece tres bloques de sistemas de IA a regular: (i) Prácticas de IA prohibidas, (ii) sistemas de IA de alto riesgo, y, (iii) sistemas de IA de uso general. Primero, los sistemas de IA prohibidos que regula el artículo 5 no pueden ser utilizados. Ahora, respecto a los sistemas de IA de alto riesgo, estos son el centro del reglamento UE de IA, ya que la norma europea dedica 43 artículos a estos sistemas, concretamente los artículos 6 a 49. En ese sentido, los sistemas de alto riesgo se definen especialmente en el capítulo III, en el cual se exige lo siguiente:

a) El cumplimiento de requisitos del artículo 8 y el establecimiento de un sistema de gestión de riesgos, de acuerdo con el artículo 9, cuestiones que sin duda recuerdan mucho a las técnicas ya consolidadas de protección de datos de carácter personal por el RGPD y que también serán clave en materia de IA (Mantelero, 2022, p.54) y en los que a buen seguro los DPDs y los responsables de seguridad tendrán mucho que aportar.
b) El cumplimiento de estándares en materia de datos y gobernanza de datos: calidad, actualización, evitando sesgos, anonimizados, limitaciones en categorías especiales, etc. Además, conforme al artículo 10, debe cumplir su relación con

(8) De hecho, la ya citada Ley 2/2025 de Galicia señala en su artículo 36.2 que "las personas que desempeñen las funciones de comisionadas de inteligencia artificial habrán de tener conocimientos técnicos, jurídicos, éticos, de normas de seguridad y de toma de decisiones automatizadas", reforzándose así la idea que en este ámbito no basta con la simple asunción por el DPD de las nuevas funciones en materia de IA.

el RGPD, donde por las razones expuestas en el apartado anterior de este artículo, los DPDs tendrán que asumir su liderazgo (UE, 2024).

c) La documentación técnica debe ser sencilla, clara, completa y comprensible de conformidad al Anexo IV, artículo 11. Para ello, se determinan obligaciones de conservación de registros, de transparencia y comunicación de información a los sujetos obligados, tratándose de obligaciones que recuerdan a las ya establecidas en el RGPD (UE, 2024).
d) En el artículo 14, indica que debe haber garantía de vigilancia humana y supervisión de los sistemas de alto riesgo (UE, 2024).
e) Bajo el artículo 15, se demanda un diseño y desarrollo de modo que alcancen un nivel adecuado de precisión, solidez y ciberseguridad y funcionen de manera uniforme en esos sentidos durante todo su ciclo de vida (UE, 2024).
f) Desde el artículo 16 a 27, se exige las obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo y de otras partes: la gestión de calidad, conservación documentación y registro, obligaciones de importadores, distribuidores, de responsables de despliegue, evaluación de impacto en derechos fundamentales (UE, 2024).

Como hemos visto en el último punto del apartado anterior, los proveedores y responsables de despliegue tienen obligación de realizar una evaluación de impacto en derechos fundamentales para la puesta en funcionamiento de sistemas de IA de alto riesgo que se deberá realizar con carácter previo a la puesta en funcionamiento del sistema (Simón, 2023, p. 55). Entre las definiciones del Reglamento UE se contiene la de "responsables de despliegue", que para la norma son "una persona física o jurídica o autoridad, órgano u organismo de otra índole públicos que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional" (p. 4, 2024). Conforme a esta definición, las Administraciones Públicas y los organismos del sector público que usen sistemas de IA de alto riesgo para el ejercicio de sus potestades (Orofino y Gallone, 2020, p.1738), cuestión problemática y que necesariamente implica labores de supervisión en materia de datos que ejercerán a buen seguro los DPDs, tendrán obligación de realizar la evaluación de impacto.

Es importante destacar que según el artículo 27 del Reglamento (UE) de IA se requiere para la evaluación de impacto:

a) Una descripción de los procesos del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista;
b) Una descripción del período de tiempo durante el cual se prevé utilizar cada sistema de IA de alto riesgo y la frecuencia con la que está previsto utilizarlo;
c) Las categorías de personas físicas y grupos que puedan verse afectados por su utilización en el contexto específico;
d) Los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y grupos determinadas con arreglo a la letra c) del presente apartado, teniendo en cuenta la información facilitada por el proveedor con arreglo al artículo 13;
e) Una descripción de la aplicación de medidas de supervisión humana, de acuerdo con las instrucciones de uso;
f) Las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, en particular los acuerdos de gobernanza interna y los mecanismos de reclamación (UE, 2024).

Se trata de un modelo de evaluación que toma claramente como inspiración el de evaluación de impacto en materia de protección de datos, y que, en cierta manera, es lógico que así sea. Pues, el Reglamento General de Protección de Datos lo articuló con la finalidad de garantizar y proteger un derecho fundamental: la protección de datos, y ahora lo que hace el Reglamento de IA es ampliar su alcance. De hecho, se ha afirmado con acierto que "si ya se realiza una evaluación de impacto de protección de datos, esta se debe llevar a cabo conjuntamente con la evaluación de impacto en derechos fundamentales" (Simón, 2023, p.55). Esto claramente sitúa al Delegado de Protección de Datos en el centro de esta nueva función vinculada a la IA, ya que si no se ocupara de ello expresamente, al menos tendría que coordinar las cuestiones relativas a la evaluación de impacto en protección de datos con la de derechos fundamentales.

8. En particular, la supervisión de *sandboxes*

Otra de las funciones que parece que van a tener los Delegados de Protección de Datos, en este caso, exclusivamente, para los que prestan sus servicios en organizaciones del sector público, es la relativa a la supervisión de *sandboxes* o entornos controlados de pruebas de interoperabilidad de datos que regula el Reglamento UE sobre la Europa Interopera-

ble. Los espacios controlados de pruebas de interoperabilidad se regulan por los artículos 11 y 12 del citado Reglamento UE. El artículo 11 se refiere a la "creación de espacios controlados de pruebas de interoperabilidad", señalando que los mismos "se gestionarán bajo la responsabilidad de las entidades de la Unión o los organismos del sector público participantes". Habrá que analizar si convendría que a nivel de cada Estado Miembro y vía aplicación de la interoperabilidad semántica en combinación con el principio de privacidad desde el diseño se realizase un tratamiento de datos en dos niveles. Por un lado, un nivel ajeno a la compartición de datos de inicio y que incluiría los documentos con datos de carácter personal y, por otro lado, estos documentos con los datos personales ya adecuadamente anonimizados, para lo cual, la participación de la persona que ostente la Delegación de Protección de Datos es imprescindible.

En el caso de que la integración fuera total y el sistema tratara datos de carácter personal y anonimizara los mismos en el momento de compartirlos, nos encontraríamos ante un supuesto de "espacios controlados de pruebas de interoperabilidad que impliquen el tratamiento de datos personales por parte de organismos del sector público", según el artículo 11. Bajo este supuesto, el artículo señala que los mismos "se gestionarán bajo la supervisión de las autoridades nacionales de protección de datos, así como de otras autoridades de supervisión nacionales, regionales o locales pertinentes". Además, en el caso de "los espacios controlados de pruebas de interoperabilidad que impliquen el tratamiento de datos personales por entidades de la Unión se gestionarán bajo la supervisión del Supervisor Europeo de Protección de Datos".

Teniendo en cuenta lo desarrollado y con estas referencias claras en la normativa UE, es inevitable que los Delegados de Protección de Datos vayan a tener que adoptar un papel necesario de supervisión y control de los entornos controlados de pruebas, por no hablar de que ya en sus funciones está la de cooperar con la autoridad de control ante procedimientos que pudieran abrirse por incumplimientos en las obligaciones derivadas de la normativa UE. Así pues, e independientemente de que nos encontremos ante entornos controlados de pruebas o *sandboxes* que traten datos de carácter personal o no, la participación del DPD en su configuración, control y supervisión parece lógica y necesaria a tenor del Reglamento sobre la Europa Interoperable. De otra parte, interesa señalar en este apartado que el artículo 11.2 del Reglamento señala que "la creación de un espacio controlado de pruebas de interoperabilidad (…)" tendrá por objeto contribuir a los siguientes objetivos:

a) fomentar la innovación y facilitar el desarrollo y la implantación de soluciones innovadoras de interoperabilidad digital para los servicios públicos;
b) facilitar la cooperación transfronteriza entre las autoridades competentes nacionales, regionales y locales y las sinergias en el ámbito de la prestación de servicios públicos;
c) facilitar el desarrollo de un ecosistema «GovTech» abierto europeo que incluya la cooperación con las pymes, las instituciones educativas y de investigación y las empresas emergentes;
d) mejorar la comprensión por parte de las autoridades de las oportunidades u obstáculos en materia de interoperabilidad transfronteriza de las soluciones innovadoras de interoperabilidad, incluidos los obstáculos jurídicos;
e) contribuir al desarrollo de soluciones de la Europa Interoperable o a su actualización;
f) contribuir a un aprendizaje normativo basado en pruebas contrastadas;
g) mejorar la seguridad jurídica y contribuir a la puesta en común de las mejores prácticas mediante la cooperación con las autoridades participantes en el espacio controlado de pruebas de interoperabilidad, con vistas a garantizar el cumplimiento del presente Reglamento y, en su caso, del resto del Derecho de la Unión y del Derecho nacional.

En la consecución de todos estos objetivos, la participación de los Delegados de Protección de Datos, gracias a su alta cualificación jurídica, puede resultar trascendental. Sin embargo, para cumplir con ello, deberán asumir su nuevo rol de liderazgo en el nuevo escenario normativo de la Unión Europea. Por su parte, el artículo 12 del Reglamento se refiere a la "participación en los espacios controlados de pruebas de interoperabilidad", y al igual que sucede en el caso anterior, se establece lo siguiente:

> En los casos en que el funcionamiento del espacio controlado de pruebas de interoperabilidad requiera el tratamiento de datos personales (…) los organismos del sector público participantes velarán por que las autoridades nacionales de protección de datos, así como las demás autoridades nacionales, regionales o locales estén ligadas al funcionamiento del espacio controlado de pruebas de interoperabilidad (RGPD, 2016).

En esa línea, el artículo 12 señala que tal escenario permite que los participantes cumplan y permitan:

> La participación en el espacio controlado de pruebas de interoperabilidad de otros agentes

> "GovTech", tales como organizaciones de normalización nacionales o europeas, organismos notificados, laboratorios de investigación y experimentación, centros de innovación y empresas que deseen poner a prueba soluciones innovadoras de interoperabilidad, en particular pymes y empresas emergentes (RGPD, 2016).

Como se observa nuevamente, las referencias al tratamiento de datos de carácter personal son constantes, así como a la supervisión de las autoridades de control, lo que determina la necesaria implicación de los Delegados de Protección de Datos. La participación en el espacio controlado de pruebas de interoperabilidad no será superior a dos años a partir de su creación, aunque podrá prorrogarse hasta un año cuando sea necesario para alcanzar el objetivo del tratamiento, según el apartado 2 del artículo 12. Además, es importante destacar el requisito que determina el apartado 3 de este artículo, ya que establece que:

> La participación en el espacio controlado de pruebas de interoperabilidad se basará en un plan específico elaborado por los participantes y tendrá en cuenta, en su caso, el asesoramiento de otras autoridades nacionales competentes o del Supervisor Europeo de Protección de Datos (RGPD, 2016).

Asimismo, en este apartado, el Reglamento determina el contenido mínimo del plan específico de la siguiente manera:

a) La descripción de los participantes y sus funciones, de la solución de interoperabilidad innovadora en cuestión y de su finalidad prevista, así como del correspondiente proceso de desarrollo, prueba y validación;
b) los aspectos reglamentarios específicos pertinentes y las orientaciones que se espera recibir de las autoridades que supervisan el espacio controlado de pruebas de interoperabilidad;
c) las modalidades específicas de colaboración entre los participantes y las autoridades, así como cualquier otro participante en el espacio controlado de pruebas de interoperabilidad;
d) un mecanismo de gestión y seguimiento de riesgos para determinar, prevenir y mitigar los riesgos;
e) los hitos clave que deberán lograr los participantes para que la solución de interoperabilidad se considere lista para su puesta en servicio;
f) requisitos de evaluación e información y posible seguimiento;
g) cuando sea estrictamente necesario y proporcionado tratar datos personales, los motivos de dicho tratamiento, una indicación de las categorías de datos personales en cuestión, los fines del tratamiento de los datos personales, los responsables y los encargados del tratamiento, así como sus funciones (RGPD, 2016).

La referencia en este punto nuevamente al Supervisor Europeo de Protección de Datos respecto al asesoramiento en la elaboración del plan específico requerirá necesariamente que ante la puesta en funcionamiento de un *sandbox* en una organización del sector público, el plan específico que hay que realizar deberá contar con el asesoramiento de la persona que ostente la Delegación de Protección de Datos.

Una cuestión importante en la regulación de los espacios controlados de pruebas es que se admite expresamente por el Reglamento en el apartado 6 del artículo 12 que los datos personales puedan tratarse en el espacio controlado de pruebas de interoperabilidad para fines distintos de aquellos para los que se recogieron inicialmente de manera lícita, pero para ello deberán cumplirse las siguientes condiciones:

a) La solución innovadora de interoperabilidad se desarrollará para salvaguardar los intereses públicos en el contexto de un alto nivel de eficiencia y calidad de la administración y los servicios públicos;
b) los datos tratados se limitarán a lo necesario para el funcionamiento de la solución de interoperabilidad que debe desarrollarse o probarse en el espacio controlado de pruebas de interoperabilidad y el funcionamiento no podrá lograrse eficazmente mediante el tratamiento de datos anonimizados, sintéticos u otros datos no personales;
c) habrá mecanismos de seguimiento eficaces para detectar la aparición de cualquier riesgo elevado para los derechos y libertades de los titulares de los datos, tal como se contempla en el artículo 35, apartado 1, del Reglamento (UE) 2016/679 y en el artículo 39 del Reglamento (UE) 2018/1725, durante la utilización del espacio controlado de pruebas de interoperabilidad, así como un mecanismo de respuesta que permita mitigar rápidamente dicho riesgo y, en su caso, detener el tratamiento;
d) los datos personales que deban tratarse se encontrarán en un entorno de tratamiento de datos funcionalmente separado, aislado y protegido, bajo el control de los participantes y serán únicamente accesibles a personas debidamente autorizadas;
e) los datos personales tratados no serán transmitidos, transferidos ni consultados de otro modo por otras partes que no sean participantes en el espacio controlado de pruebas de interoperabilidad, a menos

que esta divulgación se produzca de conformidad con el Reglamento (UE) 2016/679 o, en su caso, el Reglamento (UE) 2018/1725 y todos los participantes hayan dado su consentimiento a ella;

f) todo tratamiento de datos personales no afectará al ejercicio de los derechos de los titulares de los datos con arreglo al Derecho de la Unión en materia de protección de datos personales, en particular el artículo 22 del Reglamento (UE) 2016/679 y el artículo 24 del Reglamento (UE) 2018/1725;

g) los datos personales tratados se protegerán con las medidas técnicas y organizativas adecuadas y se suprimirán una vez concluida la participación en el espacio controlado de pruebas de interoperabilidad o cuando haya vencido el plazo de conservación de los datos personales;

h) los archivos de registro del tratamiento de datos personales se conservarán mientras dure la participación en el espacio controlado de pruebas de interoperabilidad, salvo disposición en contrario en el Derecho de la Unión o nacional;

i) se conservará y se transmitirá al Comité una descripción completa y detallada del proceso y la justificación del entrenamiento, la prueba y la validación de la solución de interoperabilidad, junto con los resultados del proceso de prueba como parte de la documentación técnica;

j) se publicará en el portal de la Europa Interoperable una breve síntesis de la solución de interoperabilidad que debe desarrollarse en el espacio controlado de pruebas de interoperabilidad, junto con sus objetivos y resultados previstos (RGPD, 2016).

En este punto, los entornos controlados de pruebas deberán cumplir los mecanismos de garantía propios del Reglamento General de Protección de Datos como la evaluación de impacto, tanto en protección de datos como seguramente también en IA, y el respecto al derecho de los titulares de datos a no someterse a actuaciones automatizadas, cuestiones todas ellas en las que la persona que ostente la Delegación de Protección de Datos necesariamente deberá intervenir.

Finalmente, una cuestión importante que interesa señalar es que existe responsabilidad de los participantes en los espacios controlados de pruebas y facultades de supervisión de las autoridades, de acuerdo con los apartados 4 y 5 del artículo 12. Bajo el mismo artículo en el apartado 7 y como ya hemos advertido constantemente a lo largo de este artículo, en materia de *sandboxes* será aplicable el Derecho de la Unión o nacional que establezcan las bases para el tratamiento de datos personales. Además, en esta línea de control, el artículo 12.8 del Reglamento (UE) 2024/903 señala lo siguiente:

> Los participantes presentarán al Comité y a la Comisión informes periódicos y un informe final sobre los resultados de los espacios controlados de pruebas de interoperabilidad, que incluirán buenas prácticas, enseñanzas extraídas, medidas de seguridad y recomendaciones acerca de su funcionamiento, así como, en su caso, sobre el desarrollo del presente Reglamento y demás Derecho de la Unión supervisados en el marco del espacio controlado de pruebas de interoperabilidad (UE, 2024).

A dicha obligación, el artículo 12.8 continúa explicando que se seguirá un dictamen que el Comité dirigirá a la Comisión "sobre los resultados del espacio controlado de pruebas de interoperabilidad en el que se especificarán, en su caso, las acciones necesarias para aplicar nuevas soluciones de interoperabilidad a fin de promover la interoperabilidad transfronteriza de los servicios públicos digitales transeuropeos". Asimismo, y en línea con el principio de transparencia, el 12.9 indica que "la Comisión velará por que la información relativa a los resultados de los espacios controlados de pruebas de interoperabilidad esté disponible en el portal de la Europa Interoperable". Es muy posible que estas obligaciones de informe, transparencia y supervisión cuando los entornos controlados de pruebas se desarrollen en organizaciones del sector público deban asumirse por algún órgano específico que pueda requerir contar con el apoyo y asesoramiento de la persona que ostente la Delegación de Protección de Datos.

9. Conclusiones

Tras el exhaustivo análisis que hemos realizado en este trabajo de investigación sobre el rol o funciones que la persona que ostente la Delegación de Protección de Datos debe asumir de conformidad a la nueva realidad normativa de la Unión Europea que se ha promulgado en los últimos años, debemos establecer cuatro conclusiones principales:

a) Los nuevos Reglamentos de la UE que regulan los datos, interoperabilidad e Inteligencia Artificial establecen que la normativa de protección de datos, es decir, el RGPD, debe cumplirse en todo caso y en sus términos, de forma que estas nuevas normas no suponen una excepción al cumplimiento de los principios y fundamentos de la protección de datos de carácter personal. Sin duda, esta circunstancia vincula a la persona

que ostente la Delegación de Protección de Datos a conocer, dominar y supervisar que esta nueva normativa y su aplicación práctica no vulneran la protección de datos.

b) Las personas que ostentan la Delegación de Protección de Datos son especialistas técnicos que desarrollan sus funciones en virtud de la normativa UE y nacional desde hace 10 años, por lo que deben tener interiorizada la supervisión, asesoramiento e informe de instrumentos como la evaluación de impacto que ahora también se ha extendido al ámbito de la Inteligencia Artificial. Este conocimiento técnico especializado determina que ante la aparición de ámbitos vinculados que utilizan herramientas derivadas de la normativa de protección de datos, las personas Delegadas de Protección de Datos sean vistas por la normativa y por las organizaciones en las que prestan servicios como las idóneas para desarrollar las nuevas funciones propias de este nuevo escenario tecnológico, social y normativo.

c) Las funciones de las personas Delegadas de Protección de Datos establecidas en la normativa UE sobre su ámbito específico se están viendo incrementadas y ampliadas en materia de datos, interoperabilidad e Inteligencia Artificial, en la línea que hemos determinado en este artículo. De hecho, ya existen normas legales, como la Ley de Galicia (España) de Inteligencia Artificial que establecen una asignación legal a las personas DPDs de las funciones que deben asumir los comisionados de IA, por lo que parece que existe una tendencia normativa en esta dirección. En estas nuevas funciones, existen dos que presentan una especial trascendencia y que hemos analizado detalladamente: (i) la evaluación de impacto en materia de derechos fundamentales en IA, y (ii) la supervisión de entornos controlados de pruebas o *sandboxes* en materia de datos e interoperabilidad, afectando esta última especialmente a las personas que ostentan la Delegación de Protección de Datos en el sector público.

d) La persona que ostente la Delegación de Protección de Datos se ha caracterizado hasta la llegada del nuevo marco normativo de datos, interoperabilidad e Inteligencia Artificial, por tener un carácter o perfil jurídico. Las nuevas funciones y/o actividades que se desprenden del nuevo escenario normativo en la UE exigen reforzar las Delegaciones de Protección de Datos con perfiles de ingeniería o técnicos, para poder desarrollar con garantías las labores de informe, asesoramiento, supervisión y control en estos nuevos ámbitos. Esto permite que las personas DPDs asuman el liderazgo de la etapa actual denominada Administración de Datos. Solo la combinación de perfiles jurídicos y técnicos en torno a una organización del dato, liderada por la persona que ostente la Delegación de Protección de Datos, permitirá el adecuado ejercicio de estas nuevas funciones que hemos analizado con detenimiento en el presente trabajo.

Esta es la situación en la que nos encontramos en la Unión Europea en estos momentos y que podría de alguna manera exportarse hacia América Latina, en general, y Perú, en particular, en un futuro no muy lejano. Este trabajo de investigación pretende poner de manifiesto esta nueva situación del rol o estatuto jurídico de la figura de la persona Delegada de Protección de Datos, tras la promulgación de las normas UE de datos, interoperabilidad e Inteligencia Artificial. Asimismo, esperamos que el presente artículo sirva para advertir sobre las necesarias reformas y cambios que deben producirse para que estas nuevas funciones puedan desarrollarse adecuadamente. Por último, esperamos que este trabajo sirva al propósito de mejorar las regulaciones futuras que en el Perú se puedan decidir, respecto a las personas que ostentan las Delegaciones de Protección de Datos, en tanto si deben aumentar sus funciones y cometidos con las nuevas regulaciones que puedan llegar de la mano del contexto tecnológico actual y la Inteligencia Artificial.

Referencias bibliográficas

Agencia Española de Protección de Datos. (2019a). *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4).* https://www.aepd.es/documento/listas-dpia-es-35-4.pdf

Agencia Española de Protección de Datos. (2019b). *Listado de tratamientos en los que no es necesario realizar una evaluación de impacto.* https://www.aepd.es/sites/default/files/2019-12/ListasDPIA-35.5l.pdf

Agencia Española de Protección de Datos. (2021). *Guía para la notificación de brechas de datos personales*. https://www.aepd.es/guias/guia-brechas-seguridad.pdf

Agencia Española de Protección de Datos (s.f.). *Gestiona RGPD*. https://www.aepd.es/guias-y-herramientas/herramientas/gestiona2

Ley 2/2025. Ley para el desarrollo e impulso de la inteligencia artificial en Galicia. 2 de abril de 2025. https://www.xunta.gal/dog/Publicados/2025/20250404/AnuncioC3B0-030425-0001_es.html

Ley Orgánica 3/2018. Ley de Protección de Datos Personales y garantía de los derechos digitales. 05 de diciembre de 2018. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Mantelero, A. (2022). *Beyond Data. Human Rights, Ethical and Social Impact Assessment*. Springer Nature. https://doi.org/10.1007/978-94-6265-531-7

Martínez, R. (2023). Reforma para una Administración de Datos. *Revista Catalana De Dret Públic*, (67), 67-81. https://doi.org/10.58992/rcdp.i67.2023.4094

Orofino, A. & Gallone, G. (2020). L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione. *Giurisprudenza Italiana*, (7), 1738-1748.

Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea*, 4 de mayo de 2016. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Reglamento (UE) 2024/903, del Parlamento Europeo y del Consejo, 13 de marzo de 2024, por el que se establecen medidas a fin de garantizar un alto nivel de interoperabilidad del sector público en toda la Unión (Reglamento sobre la Europa Interoperable). *Diario Oficial de la Unión Europea,* 22 de marzo de 2024. https://eur-lex.europa.eu/eli/reg/2024/903/oj/spa

Reglamento (UE) 2024/1689, del Parlamento Europeo y del Consejo, 13 de junio de 2024, por el que se establecen normas armonizadas sobre la inteligencia artificial y se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Ley de Inteligencia Artificial). *Diario Oficial de la Unión Europea,* 12 de julio de 2024. http://data.europa.eu/eli/reg/2024/1689/oj

Sanz, F. (2018). El delegado de protección de datos: algunas claves para su implantación en las universidades españolas. En F. López, R. Rivero, & M. Fernando (Coords.), *Organización de la Universidad y la Ciencia* (pp. 675-685). INAP.

Simón, P. (2023). Las evaluaciones de impacto algorítmico en los derechos fundamentales: hacia una efectiva minimización de sesgos. En Cotino Hueso, L., y Castellanos Claramunt, J. (Dirs.), *Algoritmos abiertos y que no discriminen en el sector público* (pp.27-56). Tirant Lo Blanch.

Universidad de Alicante (s.f.). *Delegación de Protección de Datos.* https://dpd.ua.es/

Universidad de Alicante (2025, 12 de marzo). *Instrucción conjunta de la defensoría universitaria, la delegación de Protección de Datos, el vicerrectorado de Ordenación Académica y Profesorado, el vicerrectorado de Estudiantes y Empleo y el vicerrectorado de Igualdad, Inclusión y Responsabilidad social sobre la utilización de grupos de aplicaciones de mensajería instantánea como espacio virtual universitario.* https://web.ua.es/es/vr-oacademica/normativa-y-procedimientos/instruccion-def-universitario-dpd-voap-vee-viirs.pdf

Universidad de Alicante (2025, 30 de julio). Doctrina de la Delegación de Protección de Datos. https://dpd.ua.es/es/doctrina-de-la-delegacion-de-proteccion-de-datos.html