Tecnologías y Protección de Datos en las AA.PP.

Noviembre de 2020

RESUMEN EJECUTIVO

La tecnología está cambiando la forma de trabajar de las Administraciones Públicas (en adelante, AA.PP.) y su relación con los ciudadanos buscando mejorar tiempos, facilitando la accesibilidad, simplificando trámites y ahorrando costes. Por otro lado, existe un riesgo específico asociado al tratamiento de datos personales por las AA.PP. haciendo uso de las tecnologías emergentes.

En este sentido, el presente documento pretende llevar a cabo un análisis de algunas de las tecnologías que están aplicándose en las AA.PP., para destacar algunos de sus aspectos más característicos desde el punto de vista de la protección de datos y poner de manifiesto algunos de los riesgos inherentes a su uso en cualquier tratamiento.

Este documento no pretende ser una guía para el cumplimiento de tratamientos específicos. Con este fin la AEPD viene publicando guías específicas sobre algunos de los temas que se tratarán a continuación, así como orientaciones sobre el RGPD o normativa nacional específica desarrollada, documentos a los que se hará referencia a lo largo del texto. El objetivo de este documento es destacar algunos aspectos que podrían ser más característicos del empleo de estas tecnologías en tratamientos realizados por las AA.PP.

Por lo tanto, la lista descrita de garantías de cumplimiento y riesgos a gestionar no es exhaustiva, sino una relación de aquellos aspectos básicos para tener en cuenta en cualquier tratamiento que utilice dichas tecnologías. Tampoco la lista de tecnologías emergentes es completa. El contenido de este documento es abierto y se pretende completar en versiones sucesivas en función de las aportaciones recibidas y extendiéndolo a otras tecnologías específicas con la finalidad de establecer objetivos de control del riesgo asociados a cada una de ellas.

Los destinatarios de este documento son principalmente los Delegados de Protección de Datos de las AA.PP. y aquellos empleados públicos encargados de promover, gestionar y utilizar estas tecnologías en la Administración, aunque el contenido, y sobre todo las referencias incluidas, pueden ser útiles a un público más amplio, como gestores de la empresa privada que pudieran actuar como encargados o desarrolladores para las AA.PP. así como a los propios ciudadanos, para entender cómo les afectan estas tecnologías en el marco de los servicios que les prestan las AA.PP..

En este documento se ha buscado un estilo sencillo para la redacción del texto, lo más alejado posible de la formalidad tanto en los aspectos técnicos como en los legales, para servir de introducción a aquellos que, en el sector público, se tienen que enfrentar al diseño de tratamientos que incluyan tecnologías emergentes.

Palabras clave: RGPD, administraciones públicas, eAdministración, Administración Digital, riesgos, protección de datos, privacidad, Big data, blockchain, cookies, inteligencia artificial, redes sociales, smart cities, tecnología.

En la revisión del presente documento han colaborado ASTIC (Asociación Profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información de las Administraciones Públicas), el Delegado de Protección de Datos del Parlamento de Andalucía, Junta Electoral de Andalucía y Defensor del Pueblo Andaluz, D. Iñaki González-Pol y Dña. Sara Degli Esposti, investigadora del Instituto de Políticas y Bienes Públicos del CSIC.

ÍNDICE

I. INTRODUCCIÓN

A. LA TECNOLOGÍA Y EL SERVICIO PÚBLICO

La tecnología nos invade, nos envuelve, y nos debe hacer la vida más fácil preservando, incluso enriqueciendo, nuestros derechos y libertades. Gran parte de nuestra vida personal y profesional consiste en interactuar a través de ordenadores y teléfonos móviles mediante una tecnología que nos obliga a renovarnos y desarrollar nuevas habilidades de forma continua.

La tecnología ha puesto a nuestro alcance posibilidades que antes eran inimaginables. Podemos comprar desde casa, hablar mientras nos vemos con personas que están a kilómetros de distancia, y gestionar tareas mucho más complejas y de una manera mucho más rápida que antes. Pero esta misma tecnología que, como aliado, nos facilita las cosas en nuestro día a día, cuando es mal entendida, podría resultar una amenaza para nuestros derechos y libertades. Nuestra dependencia de las máquinas y de su buen funcionamiento es prácticamente total, nunca en la historia del ser humano había habido tantas personas que supieran de nosotros y que conocieran nuestros gustos, costumbres o secretos, y nunca tampoco una persona delante de un ordenador tuvo tanto poder en sus manos para ayudar a otros o para perjudicarles.

El uso de las tecnologías de la información y comunicaciones o TIC por parte del sector público, la Administración Digital, permite ofrecer mecanismos más avanzados para implementar tanto los servicios que nos prestan como aquellos requeridos para su propio funcionamiento interno. Estos servicios son, en muchos casos, tratamientos de datos personales que se implementan haciendo uso de una o varias tecnologías aportando eficacia, eficiencia, disponibilidad, interoperabilidad y la racionalización de los recursos, entre otros beneficios.

Los gestores públicos, que llevan a cabo los tratamientos de datos personales, tienen la obligación de cumplir con la normativa en materia de protección de datos en el ámbito de su competencia, debiendo aplicar las medidas técnicas y organizativas que fueran necesarias en cada caso para garantizar, entre otros, los derechos de los ciudadanos, la transparencia y la aplicación de los principios de responsabilidad proactiva, así como el resto de los principios de tratamiento exigidos en el Reglamento General de Protección de Datos[1] (en adelante RGPD).

La adecuación de un tratamiento al RGPD requiere que cualquier paso dado en el diseño, implementación y gestión del tratamiento cuente con todas las garantías desde el origen. Expresándolo de una forma muy poco formal, es preciso responder a las siguientes cuestiones: "¿quién?" (artículos 24 y 26 sobre la responsabilidad), "¿para qué?" (artículo 5.1.b RGPD. Principio de limitación de la finalidad), el "¿por qué?" (artículo 5.1.aPrincipio de licitud y lealtad y el resto del capítulo II), "¿cuánto?" (artículo 5.1.c Principio de minimización), "¿cuándo?" (artículo 5.1.e Principio de limitación del plazo de conservación). Después vendrán el "¿cómo?" (artículo 5.2 Principio de responsabilidad proactiva, que a su vez engloba el 6.1.d y e, y los capítulos IV y V), el "¿dónde?" (artículos 28 sobre el encargado, 29 y capítulo V) y el "¿de qué manera?" en relación a los derechos de los interesados que es preciso preservar (artículo 5.1.a Principio de transparencia y el capítulo III).

Cabría la posibilidad de haber realizado una guía formal y exhaustiva tanto desde el punto de vista técnico como en los aspectos legales de protección de datos para analizar todas

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 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). https://www.boe.es/doue/2016/119/L00001-00088.pdf

estas cuestiones. De haberlo hecho así, probablemente se habría obtenido un documento más completo y muy útil para aquellas personas especializadas en la tecnología y en la protección de datos. Sin embargo, se ha apostado por realizar un documento dirigido a aquellos lectores que no conocen, ni necesitan conocer, el detalle de estas tecnologías, pero sí les interesa entender cómo funcionan y cómo pueden afectar al tratamiento de los datos. Para ellos se ha escrito un texto sencillo, buscando la claridad por encima del detalle, que les ofrezca una visión horizontal de las tecnologías y sus riesgos. No obstante, dirigido a aquellos que necesiten profundizar en alguno de los conceptos tratados, se han añadido enlaces y referencias a pie de página que permitan completar información a artículos, considerandos y documentación complementaria de interés.

B. EL RIESGO PARA LOS DERECHOS Y LIBERTADES EN LAS AA.PP.

El Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales[2] (en adelante, LOPDGDD) contemplan la posibilidad de que la introducción de tecnologías disruptivas, innovadoras o no suficientemente maduras en las actividades de tratamiento sean un factor que incremente el riesgo para los derechos y libertades de los interesados; riesgo que debe ser evaluado.

La evaluación, gestión y minimización del riesgo para los derechos y libertades es una obligación del responsable del tratamiento (artículos 23.2.g, 24.1, 25, 32, 33, 34, 35 y 36 entre otros) y forma parte de la lista de cumplimiento normativo. El RGPD, aunque da algunas indicaciones, no es concreto a la hora de identificar y pautar cómo realizar la gestión del riesgo de cada tratamiento de forma específica.

Cualquier tratamiento que se implemente en el seno de las AA.PP. conlleva una serie de riesgos que se han de gestionar como en cualquier otro proceso que se desarrolle dentro de una organización. Esta gestión no difiere de la que debe realizar cualquier otra entidad en el ámbito de sus actividades que impliquen un tratamiento de datos personales. Por ejemplo, toda entidad a la hora de poner en marcha un producto o servicio ha de gestionar, entre otros, el riesgo financiero de abordar e implementar una nueva iniciativa, el riesgo del coste que supone en relación al beneficio que aporta, el riesgo de que el nuevo servicio se pueda desplegar según un calendario, el riesgo de coste de oportunidad, el riesgo de la fiabilidad de las opciones técnicas o tecnologías a emplear, el riesgo legal de los futuros cambios normativos, el riesgo de cumplimiento que la expone a sanciones administrativas, civiles o penales, el riesgo medioambiental, el riesgo de seguridad en relación a la continuidad del sistema, el riesgo de ataques reputacionales, el riesgo de fraude, etc. Todos estos riesgos no se analizan por separado, sino que se han de analizar de forma integral[3] para alcanzar una decisión en el marco de un planteamiento holístico que tome en consideración el contexto global del tratamiento.

Formando parte de ese análisis integral se encuentra la gestión de los riesgos para los derechos y libertades de las personas. Dicha evaluación no está en relación con el riesgo de cumplimiento de los principios de tratamiento, derechos y obligaciones establecidos en el RGPD, es decir, con la evaluación de la posibilidad de incurrir en sanciones, pérdidas financieras significativas o pérdidas de reputación por incumplimiento de leyes, regulaciones, normas internas y códigos de conducta.

La gestión del riesgo para los derechos y libertades en el ámbito de un tratamiento de datos personales ha de contemplar la posibilidad de que, incluso cumpliendo formalmente con lo establecido en la normativa de protección de datos, el contexto y el alcance en el que

[2] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

[3] Norma ISO 31000:2018: Marco de trabajo para la gestión del riesgo

se realiza el tratamiento pueda introducir cierto grado de incertidumbre sobre su necesidad y proporcionalidad, así como de la eficacia y efectividad de las garantías jurídicas y técnicas aplicadas.

Hay que tener en cuenta que el tratamiento de datos personales en las AA.PP. implica riesgos distintos frente a los riesgos de un tratamiento que pueda realizar cualquier otro responsable y que se derivan, al menos, del volumen de sujetos afectados, de la extensión de los datos recogidos, de la imposibilidad, en muchos casos, de oponerse al tratamiento y del poder o asimetría inherente que existe entre las AA.PP. y los ciudadanos o interesados de los que tratan datos. Por otra parte, independientemente del hecho de que todos los tratamientos en las AA.PP. están guiados por un espíritu de servicio público, el mismo que alienta el trabajo de sus empleados, estos posibles riesgos podrían materializarse sobre los ciudadanos en determinadas situaciones, como, por ejemplo, situaciones de quiebras del estado de derecho, situaciones de abuso por parte de los responsables públicos, en circunstancias de filtrado masivo o selectivo de datos personales como consecuencia de brechas de seguridad, ante supuestos de posibles cambios legislativos incluso en terceros países a los que hubieran sido transferidos los datos, ante casos de corrupción, en situaciones de emergencia fuera de control, etc.

En consecuencia, las AA.PP., en tanto que son responsables del tratamiento de los datos de los ciudadanos, antes de poner en marcha nuevas actividades de tratamiento o modificar servicios ya prestados que hagan uso de nuevas tecnologías, deberán identificar aquellos riesgos a los que pueda estar expuesto el tratamiento. También deberán adoptar las medidas técnicas y organizativas necesarias que, desde el diseño y por defecto, permitan eliminar o al menos mitigar a un nivel aceptable, los daños que, para los derechos y libertades de las personas, pudieran derivarse del tratamiento.

Ha de tenerse en cuenta que los ciudadanos que se podrían encontrar en una situación de riesgo no son solo los administrados, sino también los propios empleados públicos en el ejercicio de sus funciones.

Es evidente que no existe el riesgo cero, tanto ignorarlo como incluso tratarlo para reducir su impacto o probabilidad de ocurrencia no lo van a hacer desaparecer. El riesgo no es estático y evoluciona de forma continua como consecuencia de la propia evolución del entorno. Es por ello por lo que, una vez identificado, exige al responsable un esfuerzo de supervisión continua y gestión permanente sobre dicho riesgo. La actitud correcta es conocer el riesgo, evaluar sus consecuencias, tomar medidas para minimizarlo y controlar su efectividad en un contexto cambiante. Este esquema de supervisión continua es lo que se define como la gestión del riesgo.

C. ESTRUCTURA DEL DOCUMENTO

En los siguientes apartados se repasan una serie de tecnologías que se han ido incorporando a las AA.PP. como medios y soporte de diferentes tratamientos de datos personales. En concreto, el documento se centra en el análisis de algunos aspectos específicos de cumplimiento y de los riesgos que pueden aparecer en los tratamientos[4] debido al empleo estas tecnologías:

- Cookies y tecnologías de seguimiento
- Redes sociales
- Cloud Computing
- Big Data

[4] A los señados en este documento, el responsable deberá analizar la casuística y riesgos, no vinculados específicamente con la tecnología empleada, que pudiera tener el tratamiento debido a otras circunstancias, derivadas de su naturaleza, ámbito, contexto y fines.

- Inteligencia Artificial
- Blockchain y Tecnologías de Registro Distribuido
- Smart Cities

En la presente edición, la selección se ha limitado a aquellas tecnologías más extensamente utilizadas o que tienen más potencial de implantación en la actualidad. En posteriores revisiones del documento podrán incorporarse nuevas soluciones tecnológicas que seguramente traerán consigo nuevos riesgos que deberán ser evaluados.

Para cada una de ellas se proporciona, en primer lugar, una breve descripción, su propósito y funcionamiento. A continuación, se señalan algunas especificidades de cumplimiento cuando las tecnologías se incorporan a un tratamiento en el ámbito de las AA.PP.. Es importante destacar que dichas especificidades de cumplimiento son aspectos concretos que se destacan con relación a la tecnología empleada, no con relación al tratamiento concreto en el que se empleen, cuyos requisitos de cumplimiento serán mucho más extensos.

Finalmente, para cada tecnología se enumeran algunos de los posibles riesgos que, en el mismo sentido que los requisitos de cumplimiento, son específicos de la aplicación de dicha tecnología, sin entrar a valorar los riesgos generales asociados al tratamiento concreto en el que se implementen. Esto último precisaría de un análisis global, completo e integral enfocado al tratamiento y, por tanto, mucho más profundo y extenso. Por otro lado, no debe pasarse por alto que algunos de los riesgos identificados y las garantías para abordarlos pueden ser comunes a otras tecnologías y, en consecuencia, extrapolar el estudio realizado y las conclusiones alcanzadas.

Este documento tiene el propósito de exponer algunos aspectos característicos de estas tecnologías con relación a la protección de datos cuando son empleadas por las AA.PP. y que vienen a complementar lo ya establecido en el RGPD, la normativa nacional y sectorial y las guías específicas ya publicadas como la Guía y listado de Cumplimento Normativo, Guía de protección de datos y Administración Local, Código de buenas prácticas en proyectos Big Data, Guía para clientes que contraten servicios de Cloud Computing,, Guía sobre el uso de Cookies, Guía de adecuación al RGPD de los tratamientos que incorporen IA, Guía de Privacidad desde el Diseño, Guía de Protección de Datos por Defecto, Guía práctica para el Análisis de Riesgos y Guía práctica para la realización de Evaluaciones de Impacto en protección de datos, Guía para la gestión de las Brechas de Seguridad, etc. Su objetivo es servir de ayuda y punto de partida para el análisis de cumplimiento y gestión del riesgo vinculado a la incorporación de tecnologías en aquellos tratamientos que, realizados en el ámbito de actuación de las AA.PP., se sustenten totalmente o hagan uso parcial de las soluciones tecnológicas descritas en este documento.

II. COOKIES Y OTRAS TECNOLOGÍAS DE SEGUIMIENTO

A. QUÉ SON LAS COOKIES

Una vez se generalizó el uso de Internet, pronto se vio la oportunidad de conocer, por ejemplo, si quien visitaba una web lo hacía por primera vez, desde dónde había llegado, por qué otras páginas del portal habían pasado los usuarios, si se habían registrado, o darles la posibilidad de guardar configuraciones o datos de una sesión. Las *cookies* permiten implementar estas funcionalidades y muchas más. Por ejemplo, las *cookies* permiten a los anunciantes conocer qué sitios de Internet visitan los usuarios para ofrecerles productos acordes a sus gustos, a los responsables de los portales les puede interesar saber también las páginas visitadas para obtener estadísticas y tomar decisiones, y un largo etcétera.

El seguimiento de la actividad de los usuarios en la red se implementa mediante dispositivos[5] que genéricamente se denominan *cookies*. Esta es una estrategia utilizada por los servidores para almacenar y recuperar información del dispositivo de un usuario, lo que permite tratar datos personales de este cuando navega e interacciona con las diferentes aplicaciones y contenidos desplegados en la Red. En realidad, bajo la denominación de *cookies* se enmarcan muchas técnicas que permiten el seguimiento de los usuarios de forma activa o pasiva, muchas veces de forma poco transparente. Entre estas tecnologías de seguimiento se pueden encontrar aquellas que utilizan las características del dispositivo, los identificadores únicos y los hábitos de navegación del usuario. Cada vez que pedimos una página, una imagen o un contenido a un servidor web, le estamos comunicando, al menos, nuestra dirección IP, con lo que se puede saber nuestra ubicación geográfica[6], pero también el modelo de navegador que usamos y, en consecuencia, también nuestro sistema operativo, el dispositivo con el que nos conectamos, y cómo está de actualizado. Un servidor web puede saber si el usuario que navega tiene un bloqueador de elementos emergentes, cuánta memoria tiene su equipo, qué tarjeta gráfica usa, o cómo mueve el ratón por la pantalla. Toda esta información se agrupa bajo el nombre genérico de *fingerprint*[7] o huella digital del dispositivo y puede utilizarse en servidores de Internet para vincular toda la actividad del usuario y así poder crear un perfil de este.

El RGPD se pronuncia respecto de las *cookies* en su considerando 30[8], reconociendo su capacidad para elaborar perfiles de las personas e identificarlas[9]. La normativa especial que regula, para los servicios de la sociedad de la información, la utilización de *cookies* viene recogida en el artículo 22.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico (LSSI)[10]. Los criterios de la AEPD para la adecuación a la normativa sobre *cookies* a los prestadores de servicios de la sociedad de la

---

[5] Se utiliza el término "dispositivo" en la normativa española como traducción de la palabra inglesa "device" utilizada en la Directiva 2002/58/EC o Directiva de ePrivacy. La extensión semántica de la palabra "device" incluye: artefacto, estrategia, artilugio o recurso.

[6] What is GeoIP and its benefits? https://serverguy.com/news/what-is-geoip/

[7] La AEPD ha publicado en septiembre de 2019 una guía llamada Fingerprinting o Huella digital del dispositivo, que está disponible en https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf

[8] *"Las personas físicas pueden ser asociadas a identificadores en línea […] como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores […]. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas."*

[9] La Comisión Europea trabaja sobre una propuesta de Reglamento del Parlamento Europeo y el Consejo sobre el respecto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas, más conocida como Propuesta de Reglamento ePrivacy https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=ES, que derogaría la Directiva 2002/58/CE

[10] Ley 34/2002, de servicios de la sociedad de la información y del comercio electrónico https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

información se encuentran detallados en la Guía sobre el uso de las cookies[11] que se publicó en noviembre de 2019 y se actualizó en julio de 2020. En dicha guía se incluyen, también, las definiciones de los distintos tipos de *cookies*, las obligaciones de los editores en cuanto a la información a proporcionar a los usuarios, el modo de recoger el consentimiento previo a su empleo y la responsabilidad de las partes en la utilización de las *cookies*. El presente documento, con relación a estos temas, se remite a dicha guía y en el apartado siguiente se atenderán a ciertas peculiaridades del uso de *cookies* por parte de las AA.PP.

B. LAS COOKIES Y LAS AA.PP.

La aplicabilidad de la LSSI

Los sujetos obligados por la normativa especial que regula las *cookies* son los prestadores de servicios de la sociedad de la información, entendidos estos como "*toda persona física o jurídica que proporciona servicios prestados normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario, así como aquellos servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios*" [12].

Tal y como se explica en la página sobre la Ley de Servicios de la Sociedad de la Información[13] del Ministerio de Asuntos Económicos y Agenda Digital:

> *En general, la LSSI no se aplica a las Administraciones Públicas, puesto que éstas no tienen el carácter de prestador de servicios de la sociedad de la información definido en su anexo. De esta forma, determinadas actividades típicas de las Administraciones, como la gestión electrónica de la recaudación de tributos o la información sobre los servicios de un tercero (como podría ser la mera información en la página web de un Ayuntamiento sobre las casas rurales existentes en el término municipal) se consideran como actividades públicas o de interés general distintas a la "actividad económica" a la que se refiere la LSSI.*
>
> *Sin embargo, cuando la actividad de una Administración sí tenga un carácter económico (por ejemplo, la venta de libros turísticos por una entidad pública dependiente de un Ayuntamiento), le será aplicable la LSSI.*

Es decir, bajo esta aproximación y con carácter general, una Administración Pública que dispone de un portal web, por el hecho de tenerlo no sería necesariamente considerada como un proveedor de servicios de la sociedad de la información y, en consecuencia, como un sujeto obligado de la LSSI. Solo podrá considerarse como tal si ofrece un *"servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario"*, por ejemplo, si en un dominio perteneciente a una Administración Pública se presta algún tipo de servicio que implique una actividad económica, como la venta de libros, entradas, etc. En ese caso, sí le será de aplicación la LSSI para aquellos dominios concretos en los que se lleve a cabo dicha actividad económica.

---

[11] Está disponible en https://www.aepd.es/media/guias/guia-cookies.pdf. Otras autoridades de países de nuestro entorno también han publicado guías recientemente como el ICO británico (https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/), la CNIL francesa (https://www.cnil.fr/en/cookies-and-other-tracking-devices-cnil-publishes-new-guidelines) o la Conferencias de Autoridades de Protección de Datos alemana https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf . Hay una interesante comparativa en https://iapp.org/resources/article/ico-and-cnil-revised-cookie-guidelines-convergence-and-divergence/. La guía sobre el uso de las cookies publicada por la AEPD ha sido actualizada para adaptarla a las nuevas Directrices sobre consentimiento revisadas por el Comité Europeo de Protección de Datos en mayo del 2020, siendo necesario la adaptación a estos nuevos criterios, a más tardar, el 31 de octubre del 2020.

[12] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico, o LSSI.

[13] http://www.lssi.gob.es/la-ley/Paginas/preguntas-frecuentes.aspx?Faq=%C3%81mbito+de+aplicaci%C3%B3n

Por otro lado, la misma definición de servicio de la sociedad de la información detalla: *"el concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios…"*. Es habitual que en una página web se encuentren componentes embebidos de terceros, herramientas y aplicaciones como redes sociales (Twitter, Facebook, etc.), canales de distribución de contenidos (Youtube, Vimeo, etc.), u otros servicios como mapas o traductores que implican la utilización de *cookies* de seguimiento, análisis o publicidad. El permitir el uso de dichas *cookies* a cambio de la posibilidad de poder incluir dichos servicios en el portal web podría constituir una actividad económica siempre que dichas herramientas o aplicaciones se ejecuten embebidos en el propio dominio de la Administración Pública y no sean enlaces a páginas de terceros. Bajo estas circunstancias, los organismos de las AA.PP. que hagan uso de servicios de terceros que impliquen el uso de *cookies* deberán de aplicar las obligaciones y garantías establecidas en la normativa especial y las guías de la AEPD.

Siempre que se incluyan cookies de terceros, también cuando se proporcionen los medios que permitan el tratamiento de datos personales por terceros[14], ya sea en los casos anteriores u otros casos tales como permitir la utilización de cookies analíticas de tercera parte, la Administración Pública ha de ser diligente a la hora de identificar que tienen lugar estos tratamientos y de garantizar que se cumplan los deberes de información y obtención del consentimiento de los usuarios.

En cualquier caso, cuando la Administración Pública no sea sujeto obligado por la LSSI, siempre que el tratamiento realizado a través de las *cookies* implique datos de carácter personal, este estará sometido al RGPD y toda la normativa de protección de datos aplicable. No obstante, las AA.PP., por razones de transparencia, podrían facilitar información sobre las *cookies* utilizadas cuando no sea necesaria la obtención del consentimiento. Para abordar las obligaciones correspondientes, las AA.PP. pueden hacer uso de las orientaciones descritas en la Guía sobre el uso de las cookies publicada por la AEPD anteriormente referenciada.

Uso de cookies en portales y apps oficiales

Los portales web de las organizaciones no son, generalmente, un conjunto de páginas estáticas de contenido fijo, sino que generalmente se apoyan en un programa gestor de contenidos (en sus siglas CMS o Content Management System[15]). Estos gestores se ejecutan en el servidor web y construyen, de manera dinámica, las páginas que le solicitan los usuarios a partir de piezas de contenido guardadas en una base de datos. Hay portales que usan gestores construidos a medida, pero la mayoría emplean programas comerciales o de código abierto. Estos gestores pueden estar usando *cookies* para su funcionamiento, de manera que el portal oficial puede requerir el uso de *cookies* como prerrequisito tecnológico. El empleo de *cookies* se puede extender a medida que se van incorporando *plugins* para aumentar la funcionalidad y características del CMS. Igualmente sucede con las apps o aplicaciones móviles que distribuyen algunas AA.PP. Normalmente, estas se construyen sobre un entorno de programación comercial o de código abierto[16], e incluyen SDKs[17] de terceros que permiten incorporar funcionalidad de forma rápida y ágil, pero que

[14] Ver técnicas como Cookie Syncing o CNAME Cloaking en el apartado de riesgos.

[15] La Wikipedia tiene una página muy completa sobre los CMS, en la que se incluyen referencias a los más usados en https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_contenidos

[16] La Wikipedia en inglés les dedica un artículo https://en.wikipedia.org/wiki/Mobile_development_framework

[17] Un kit de desarrollo de software (o SDK, del inglés Software Development Kit) es un conjunto de herramientas de desarrollo de software que permite a un desarrollador crear una aplicación informática para un sistema concreto. Suelen incluir una interfaz de programación de aplicaciones (o API), un entorno de desarrollo integrado (o IDE) y otras utilidades, incluidos códigos de ejemplo, notas técnicas y documentación de soporte para ayudar al programador a desarrollar su tarea.

también pueden estar incorporando la utilización de *cookies*[18] adicionales u otras técnicas de seguimiento, como el tratamiento de identificadores únicos de publicidad[19].

Ante estas circunstancias, el responsable del portal oficial debe informarse, y en su caso comprobar, qué tipo de *cookies* requiere el gestor de contenidos y los *plugins* que se van a utilizar. En su caso, el responsable ha de tomar las medidas necesarias para eliminar aquellas no necesarias para la prestación del servicio, optando por aquellos gestores de contenidos que hacen uso de las *cookies* técnicas propias. De igual modo, en el caso de las aplicaciones móviles deben tomarse precauciones análogas[20], sobre todo con relación a las técnicas de seguimiento que en dicho entorno son más utilizadas, para evitar que se incorporen tratamientos de datos personales no legítimos a través de los SDKs de terceros. Además de establecerlo como requisito de contratación y exigirlo a sus proveedores, este comportamiento debería de ser auditado por el responsable para verificar que se respeta.

Por otro lado, en ningún caso el rechazo al uso de las *cookies* no imprescindibles para la implementación del servicio puede suponer un impedimento para el acceso al portal de la Administración Pública, ni mucho menos limitar o impedir su acceso al ejercicio de derechos y libertades. Con relación a esto, hay que tener en cuenta que el uso de determinadas tecnologías, por sus requerimientos específicos, pueden dificultar la navegación y el acceso a contenidos relevantes a usuarios que, libremente, deciden no aceptar las *cookies* o que, por el equipamiento tecnológico del que disponen o por limitaciones en este (hay muchos usuarios que navegan con equipos desactualizados, móviles de limitada funcionalidad o que tienen que emplear ayudas de accesibilidad o dispositivos adaptados), no soportan el uso de dichas tecnologías. En este contexto, es importante tener en cuenta, a la hora de diseñar tanto los portales o las aplicaciones móviles del sector público como los contenidos que sirven, que las AA.PP. están obligadas a cumplir con el Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público[21] [22].

En todo caso, si se opta por recurrir a esta tecnología para realizar un análisis de tráfico, aunque sea de forma parcial para medir, por ejemplo, el interés de los usuarios por determinadas secciones de un portal web, es conveniente seguir el principio de minimización de datos[23] y recoger los datos de navegación de forma anónima o seudónima, estableciendo medidas[24] que permitan perder el vínculo con cualquier información personal o, al menos, minimizarlo.

Por último, si se recurre a herramientas de terceros para realizar un análisis del tráfico web y recoger información sobre la frecuencia de visitas de los usuarios o el tiempo que dedican a la navegación, han de estudiarse las distintas alternativas que ofrece el mercado,

[18] Hay que subrayar que las cookies técnicas que permiten el funcionamiento y dar el servicio web están exentas de los deberes establecidos en la LSSI y que forman parte del tratamiento legitimado.

[19] Control de usuarios en la personalización de anuncios: https://www.aepd.es/sites/default/files/2019-12/nota-tecnica-android-advertising-id.pdf

[20] El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf

[21] Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12699

[22] El Portal de Administración electrónica ha incorporado materiales en relación con las principales novedades que incorpora el RD 1112/2018 con respecto a la anterior normativa y, en particular, un resumen dirigido a las entidades obligadas, públicas y privadas, que tienen que aplicar los requerimientos del RD 1112/2018 (https://administracionelectronica.gob.es/pae_Home/dam/jcr:21516ff3-7f1e-4db1-b46a-889014a9ddea/2020-03-27-Resumen_AAPP_RD-1112-2018_v_2_0.pdf) y el enlace al estándar de aplicación para el cumplimiento de los requisitos (https://www.etsi.org/deliver/etsi_en/301500_301599/301549/02.01.02_60/en_301549v020102p.pdf)

[23] Artículo 5.1.c del RGPD – Principios relativos al tratamiento. Principio de minimización.

[24] Una posible medida puede ser, por ejemplo, reducir la dirección IP de navegación al último rango de dígitos.

analizando sus características técnicas, modo de funcionamiento[25] y opciones de configuración para evitar caer en posibles incumplimientos normativos.

Uso tecnologías de seguimiento en componentes de terceros

Como se exponía en la sección anterior, en muchas ocasiones los portales y las aplicaciones móviles son un gran contenedor o estructura del que cuelgan elementos proporcionados por terceros proveedores. Cuando se navega por las páginas de Internet, en realidad se está accediendo a múltiples componentes como imágenes, videos embebidos, fuentes de letras, estilos, anuncios, contadores estadísticos[26], widgets de redes sociales o *plugins* diversos que están distribuidos en múltiples servidores de terceros, y cada uno de ellos puede instalar su cookie o anotar nuestra visita. Cuando las AA.PP. construyen sus servicios utilizando dichos componentes han de auditar si estos hacen uso de tecnologías de seguimiento, no solo cuando se diseña el sistema, sino durante el tiempo de explotación (ciclo de vida del sistema y del tratamiento) y estar muy atentos a la aparición de estos posibles elementos de seguimiento en las actualizaciones de sus portales oficiales, pero también en los mensajes de correo electrónico con HTML[27] o imágenes[28], hilos de noticias RSS[29] o cualquier otro producto[30].

C. RIESGOS PARA LOS DERECHOS Y LIBERTADES ASOCIADOS AL USO DE COOKIES

Uno de los principales riesgos del uso de *cookies,* u otras tecnologías de seguimiento, es la recopilación de información personal más allá de lo necesario para el propósito del tratamiento, especialmente con relación a las categorías especiales de datos, ya sea de forma directa o indirecta, o bien proporcionar los medios para que terceros lo hagan. Por ello, es necesario evaluar, incluso para las *cookies* técnicas, hasta qué punto su uso puede determinar una recogida o inferencia de información adicional del sujeto y tomar las medidas adecuadas para minimizar dicho riesgo.

Esta circunstancia será más grave cuando las tecnologías de seguimiento sean utilizadas por terceros, como es el caso de tecnologías de seguimiento empleadas por componentes incrustados en la página web o en una aplicación móvil de la Administración. Esto puede ocurrir incluso de forma indirecta cuando las páginas web o las apps se construyen haciendo uso de elementos como tipos de letras servidos por terceros, imágenes, mapas, herramientas u otras aplicaciones. También cuando, para facilitar la disponibilidad de la página, el contenido se encuentre distribuida entre múltiples servidores que no pertenecen al responsable.

Hay que tener en cuenta los riesgos en el uso de herramientas para la implementación de los sitios web, como los CMS antes citados, ya que suelen actualizarse dinámicamente. Las configuraciones pueden variar entre versiones, derivadas de actualizaciones automáticas y, en algunos casos, estas no están sometidas a un control previo de calidad,

[25] Por ejemplo, la herramienta Google Analytics resulta especialmente problemática en cuanto a los estándares de protección de datos, pues las direcciones IP de los usuarios se almacenan en servidores ubicados en los Estados Unidos y la reciente sentencia del Tribunal de Justicia de la Unión Europea ha declarado inválido el acuerdo de "Escudo de Privacidad" que existía entre la UE y EE.UU. (Decisión 2016/1250 sobre la adecuación dela protección conferida por el Escudo de la privacidad UE-EE. UU.).

[26] Cookies e identificación de usuarios https://developers.google.com/analytics/devguides/collection/analyticsjs/cookies-user-id?hl=es-419

[27] HTML son las siglas de Hyper Text Markup Language, el lenguaje de las páginas web. https://es.wikipedia.org/wiki/HTML

[28] Se conoce como Pixel de seguimiento https://es.ryte.com/wiki/P%C3%ADxel_de_Seguimiento

[29] RSS son las siglas de Really Simple Syndication, un protocolo de agregación de noticias, cuyo uso ha bajado notablemente en los últimos años por la presencia de la red Twitter como medio de redifusión. https://es.wikipedia.org/wiki/RSS

[30] Existen algunas páginas en Internetque permiten visualizar de forma gráfica este 'árbol de llamadas' que se produce cuando mostramos una página web. Como ejemplo podemos citar https://webbkoll.dataskydd.net/en/ o https://requestmap.webperf.tools/.

por lo que pueden incluir nuevas cookies o componentes de terceros que realicen tratamientos adicionales. Por lo tanto, las actualizaciones o cambios han de estar documentados, sometidos a comprobaciones previas a su puesta en producción y, como precaución, limitarse a aquellas nuevas versiones que tengan mejoras contrastadas en temas de interés para el tratamiento, como puede ser mejoras de seguridad.

Un elemento para gestionar dicho riesgo, aunque no el único, es realizar auditorías periódicas de los componentes, el tipo de datos tratados, el destino del tráfico generado por las aplicaciones, el grado de vinculación de dicha información con las operaciones del usuario en las AA.PP., así como un análisis de las inferencias adicionales y efectos colaterales que se podría realizar sobre el administrado.

Para el caso en el que la Administración Pública proporcione servicios en los que no existe la necesidad de identificar al usuario, o que incluso es recomendable que no haya identificación, como servicios de asesoría a menores o víctimas, consultas de salud, buzones anónimos de denuncia, etc., hay que analizar el riesgo de reidentificación, perfilado o registro del histórico de navegación que supone el uso de *cookies* y otras tecnologías de seguimiento.

Técnicas conocidas como Cookie Syncing[31] y CNAME Cloaking[32] permiten disfrazar cookies de tercera parte como cookies de primera parte en el navegador del usuario, lo que supone un riesgo directo para la protección de datos al permitir que se eviten los controles establecidos en los navegadores web para limitar las cookies de terceros o el seguimiento.

Finalmente, hay riesgos de seguridad en relación con las cookies que pueden afectar a la protección de datos como pueden ser la captura de información de autenticación en canales inseguros y secuestro de sesión, técnicas de *cross-site scripting* (XSS), uso de cookies maliciosas inyectadas por subdominios (*cookie tossing*), etc. Este tipo de ataques evolucionan en el tiempo e implican la necesidad de reevaluar la robustez del portal web en función del estado del arte.

[31] What is Cookie Syncing and How Does it Work? (https://clearcode.cc/blog/cookie-syncing/)
[32] Characterizing CNAME cloaking-based tracking (https://blog.apnic.net/2020/08/04/characterizing-cname-cloaking-based-tracking/)

III. REDES SOCIALES

A. QUÉ SON LAS REDES SOCIALES

Las redes sociales son uno de los canales de información más usados en Internet. De hecho, con la televisión (72%) y las webs y aplicaciones de periódicos (44%), las redes sociales (53%) son los medios que más usan los internautas para informarse[33].

En las redes sociales la información contenida puede ser de varios tipos:

- Publicaciones de documentos, textos, fotografías, videos, enlaces, datos de actividad física, etc.
- Comentarios y respuestas a las publicaciones, formando un hilo de diálogo entre publicadores y lectores.
- Perfiles de usuarios, que pueden ser tanto personas físicas como organizaciones. Contienen información personal y de contacto, así como el histórico de sus publicaciones y con qué otros elementos de la red se relacionan[34] (amigos, seguidores, etc.). Las redes sociales ofrecen diferentes mecanismos de protección de los contenidos de sus usuarios.

Los usuarios encuentran en las redes sociales un canal sencillo, accesible e inmediato por el que pueden compartir contenidos, socializar o incluso ofrecer un escaparate para dar a conocer sus productos o servicios, generalmente sin coste (o incluso recibiendo dinero por sus publicaciones, como en el caso de los *influencers*[35]). En las redes sociales se produce un tratamiento que va más allá del puro intercambio de contenidos entre usuarios y que permite monetizar (ganar dinero) la actividad de la red social. Por un lado, la red social perfila los usuarios para publicar anuncios personalizados que, por estar adaptados a sus gustos y características, tienen un impacto muy alto. Por otro lado, podría vender los datos de los usuarios a empresas o instituciones interesadas en perfilar a sus clientes y potenciales clientes para ofrecerles productos o servicios por otros canales. Estos tratamientos se legitiman, normalmente, bien por el consentimiento del usuario o bien en el marco de la ejecución de un contrato con o sin contraprestación económica.

Para publicar, y a veces para acceder a los contenidos en una red social, es necesario darse de alta como usuario. Dependiendo de la red social, puede ser obligatorio que el usuario se identifique con una identidad real, evitando así que el usuario pueda darse de alta de forma anónima, con seudónimos[36] o que pueda disponer de distintas cuentas con varias identidades. Otras redes, sin embargo, preservan el anonimato de sus usuarios al menos a la hora de registrase.

Dentro de las redes sociales, las normas de publicaciones aceptables o etiqueta son establecidas por el proveedor del servicio, que generalmente se apoya en una comunidad o estructura participativa[37]. Las redes sociales, para los usuarios europeos, están sometidas a la legislación de la Unión Europea (UE), como el RGPD, y a las legislaciones vigentes donde están sus usuarios. Esta competencia múltiple crea a veces tensiones entre los

[33] Informe Digital News Report de 2019 (http://www.digitalnewsreport.es/2019/el-45-de-los-usuarios-elige-la-television-como-medio-principal-para-informarse-mientras-el-40-opta-por-las-fuentes-online/)

[34] El Blog de la AEPD contiene un artículo titulado ¿Cuánto sabe Facebook sobre mí? https://www.aepd.es/es/prensa-y-comunicacion/blog/cuanto-sabe-facebook-sobre-mi

[35] El término no existe aún en castellano. Si miramos su significado en inglés en https://dictionary.cambridge.org/es/diccionario/ingles/influencer :*someone who affects or changes the way that other people behave/ a person who is paid by a company to show and describe its products and services on social media, encouraging other people to buy them*

[36] https://www.cnet.com/news/facebook-took-down-more-than-3-billion-fake-accounts/ En mayo de 2019 Facebook estimaba que un 5% de sus cuentas activas eran falsas. Por su parte, Twitter limpió 70 millones de cuentas falsas en 2018 (https://www.bbc.com/news/technology-44682354)

[37] Como ejemplos podemos citar los Facebook Community Standards (https://www.facebook.com/communitystandards/)

proveedores y las autoridades nacionales, por ejemplo, cuando se trata de retirar contenidos sobre una persona concreta[38], noticias falsas, o contenidos que atentan contra los derechos de minorías o colectivos con vulnerabilidades especiales.

En cuanto a los datos personales tratados en la interacción con la red social, hay que tener en cuenta que no sólo se tratará de la información asociada al perfil del usuario que accede a la red, sino también la generada en la interacción con el contenido publicado (que dependiendo del tipo de red social podrán ser "me gusta", iconos de reacción al contenido, etiquetas de clasificación, sellos de tiempo, reenvíos o republicaciones, comentarios, etc.) de información general de navegación que incluyen la posible recogida de datos como: páginas visitadas, direcciones IP u otra información de localización, *fingerprint* del dispositivo, del navegador y cookies.

La interacción con la red social también se puede realizar desde el sitio web de un tercero mediante la inclusión de widgets de redes sociales. Estos widgets suelen ser iconos que enlazan a una red social. Detrás de los widgets existen cookies y otros mecanismos de tratamiento de información de navegación, como lo explicado anteriormente, y además las cookies y mecanismos de tratamiento de información relacionados con la interacción específica en la página del tercero en la que se encuentra el widget.

B. LAS REDES SOCIALES Y LAS AA.PP.

Aspectos generales

A diferencia de los sitios web gestionados directa o indirectamente por las propias AA.PP. y sobre los que es posible un control total del contenido y del tipo de servicio prestado, la red social es un entorno que no está pensado inicialmente para el uso administrativo y que, en general, no se adapta a él. En cualquier caso, supone un tratamiento que tiene que cumplir con lo establecido en el RGPD.

En ocasiones las redes sociales se utilizan como un vehículo para hacer eco de la información oficial (republicación o enlace) y al mismo tiempo para proporcionar información ágil a los usuarios como se haría, por ejemplo, por un canal telefónico o una ventanilla de información[39]. En este escenario, el papel que juegan los *community managers* o administradores de las redes sociales es muy importante. Ellos son los que generan contenido de interés para la ciudadanía en relación con el ámbito competencial de la Administración, y los que dan respuesta a las cuestiones que llegan a través de este canal. El trabajo de los *community managers* siempre debe enmarcarse en los objetivos definidos por el organismo, en el marco de una estrategia de comunicación[40], y estos han de ser conscientes de la obligatoriedad de aplicar la normativa de protección de datos.

La relación de las AA.PP. con las redes sociales puede tomar muchas formas. La más conocida sería la presencia de perfiles 'oficiales' de los organismos en redes sociales

[38] Cuando hablamos de retirar los contenidos que afectan a una persona solemos referirnos al derecho al olvido. La AEPD cuenta con una página con más detalles sobre su ejercicio en https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido

[39] Varios ministerios y AA.PP. en España cuentan con su página en Facebook, como el Ministerio de Sanidad: https://www.facebook.com/MinSanidad/. La propia Guía de Comunicación Digital para la Administración General del Estado (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Guia_de_Comunicacion_Digital_para_la_Administracion_General_del_Estado.html) en su fascículo 8 da buenas indicaciones para orientar la presencia en las redes sociales de las Administraciones. Por otro lado la Guía de redes sociales de la Generalitat de Cataluña (http://atenciociutadana.gencat.cat/ca/serveis/xarxes-i-missatgeria-instantania/xarxes-socials/guies-i-normativa/guia-de-xarxes-socials/) es otro recurso útil para las Administraciones.

[40] La Guía de Comunicación Digital para la Administración General del Estado proporciona un marco de criterios, recomendaciones y buenas prácticas a tener en cuenta por sus Departamentos y organismos al crear, generar contenidos o evolucionar los sitios y portales web, las sedes electrónicas o los sitios relacionados con las nuevas tecnologías web2.0 (blogs, cuentas o perfiles de redes sociales a los que accede bajo los nombres oficiales de los Departamentos u organismos de la AGE).

abiertas o comerciales, aunque no pueden obviarse otros usos como las redes sociales cerradas utilizadas como vehículo de comunicación interna, las redes o grupos no oficiales de empleados, los empleados que publican en redes sociales a título individual, y por último podríamos incluso hablar de la aparición y referencia a las Administraciones en perfiles, publicaciones o comentarios de terceros.

Uso de las redes sociales de forma interna

Las Administraciones pueden usar las redes sociales internamente o para relacionarse con el público en general. En el uso interno podemos encontrarnos con redes cerradas, pensadas para los empleados como una evolución de las intranets corporativas a las que se han añadido rasgos sociales[41]. Estas redes se apoyan en paquetes de software específicos y el acceso está restringido o incluso prohibido a terceros.

Otro posible uso interno de las redes sociales es el que resulta de las comunicaciones informales de los empleados, que forman grupos para dialogar o intercambiar mensajes y noticias como lo harían de forma informal en los pasillos de la organización. Este tipo de redes a veces surge de forma espontánea y otras veces puede ser promovido por las propias organizaciones para crear un vínculo entre sus empleados. Nos podemos encontrar con empleados de una misma organización (y a veces también junto con exempleados y externos) que hablan entre ellos a través de una red insegura sin ser, muchas veces, conscientes de ello. Un empleado, de manera inconsciente y sin valorar los riesgos que representa, puede llegar incluso a confundir la red social de compañeros con la intranet o los canales internos establecidos y publicar documentos, estrategias o datos corporativos que pueden ser accesibles, e incluso fácilmente copiados, por terceros no autorizados. A su vez, este empleado también puede publicar opiniones o hacer comentarios de tipo eminentemente personal que un lector malintencionado podría hacer pasar por oficiales. En este mismo contexto y estrechamente relacionado, la AEPD se ha hecho eco en diversas ocasiones del peligro que pueden representar los grupos de empleados y los comentarios vertidos en ellos en situaciones de acoso laboral, sexual y casos de discriminación[42].

En la Política de Información de la entidad han de estar definidos claramente los límites de usos de redes sociales fuera del entorno estrictamente personal, así como el uso de los BYOD *(Bring Your Own Device)*. Si en la política se admiten este tipo de canales de comunicación, se está admitiendo un tratamiento del que será responsable la entidad y, por lo tanto, habrá de cumplir con los establecido en el RGPD y en el ENS (Disposición adicional primera de la LOPDGDD).

Empleados que publican en redes sociales de forma individual

Las redes sociales han dado a muchas personas la posibilidad de compartir su conocimiento o sus ideas, de forma anónima o usando su nombre real. Estas personas han creado una especie de marca personal en la que el prestigio se mide en seguidores, enlaces y citas. En los casos más exitosos tenemos los llamados *influencers* que han hecho su fama alrededor de la publicación, en las redes sociales, de sus opiniones y juicios.

Sin llegar a estos extremos, es bastante común que profesionales de todos los sectores publiquen contenidos en redes sociales aportando su experiencia al conocimiento común. En algunas empresas es frecuente incluso que se promueva el uso de las redes sociales por los expertos de la organización como una forma de promoción[43], especialmente en redes

[41] Como ejemplos podríamos citar IBM Notes, Jive o Ms Sharepoint

[42] La AEPD elaboró un documento sobre protección de datos, como garantía en las políticas de prevención del acoso. Puede descargarse en https://www.aepd.es/sites/default/files/2019-11/191107-recomendaciones-sobre-acoso-digital-aepd_0.pdf

[43] 5 maneras de convertir a los empleados en defensores de tu marca en Twitter https://business.twitter.com/es/blog/employees-advocates-on-twitter.html

sociales donde la intención es compartir la experiencia laboral del empleado. Sin embargo, que los empleados publiquen información profesional puede infringir los principios de protección de datos, cuando se incluye información personal y se carece de legitimación[44].

En la Política de Información de la entidad ha de quedar claro, al menos desde la perspectiva de protección de datos, la prohibición de realizar el tratamiento de datos personales relativos a la actividad de la entidad a través de los perfiles personales en las redes sociales de los empleados, quedando los empleados que realicen ese tratamiento ilegítimo como responsables del tratamiento.

El uso de redes sociales por AA.PP. para ofrecer servicios a los ciudadanos

Cuando una Administración Pública decide ofrecer información o servicios a los ciudadanos a través de una red social, no se puede obligar al administrado a contar con perfiles en la misma, en la medida en que estas redes realicen tratamientos adicionales de datos basados en el consentimiento del usuario.

De acuerdo a los Considerandos 42 y 43 y el propio artículo 7 del RGPD, para que un tratamiento basado en el consentimiento sea lícito, el consentimiento prestado ha de cumplir una serie de condiciones[45], en concreto ha de ser informado, específico, libre e inequívoco además de no prestarse en condiciones en las que exista un claro desequilibrio entre el interesado y el responsable del tratamiento. En el caso de que la Administración proporcionase dicho canal como único medio para un servicio, sin proporcionar canales alternativos a través de los cuales este pueda ser prestado en un plano de igualdad, el consentimiento no podría ser considerado libre, además de suponer un obstáculo[46] para aquellos ciudadanos más afectados por la brecha digital ante la imposibilidad de acceder a la información proporcionada o ejercer los derechos que les asisten.

Por ejemplo, el realizar iniciativas de participación ciudadana únicamente a través de redes sociales obliga a aquellos sujetos que quieran tener influencia en dicha iniciativa a consentir en el tratamiento de un tercero y, en consecuencia, a otorgar un consentimiento que no cumplirá los requisitos que exige el RGPD.

El servicio proporcionado a través de la red social deberá cumplir con todas las obligaciones establecidas en el RGPD, entre ellas el deber de informar. Esta obligación podría implementarse en un post fijado al inicio de la cuenta de forma que el usuario pueda acceder fácilmente y que proporcionase la política de privacidad o un enlace a la misma.

Un caso especial es la implementación de servicios en redes sociales orientados específicamente a menores[47]. En estas situaciones, cuando la actividad en la red social implique tratamiento de datos de menores de 14 años hay que garantizar que el consentimiento para el tratamiento de los datos ha sido prestado por los padres o tutores del menor.

El tratamiento de los datos por parte de las redes en la que los usuarios disponen de cuenta se basará, en general, en aquellos necesarios para la ejecución del contrato de servicio o en el consentimiento prestado. Hay que distinguir dichas causas de legitimación de las de aquellos tratamientos de los datos de los ciudadanos realizados por las AA.PP. con perfil en las redes sociales derivados de la interacción con las personas a raíz de la

[44] Artículo 5.1.a) del RGPD - Principios relativos al tratamiento. Principio de licitud, lealtad y transparencia
[45] Artículo 7 del RGPD - Condiciones para el consentimiento
[46] El artículo 14 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común, establece el derecho de las personas físicas de elegir en todo momento si se relacionan con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos, salvo en los supuestos en que estén obligadas a relacionarse de esta manera. https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20200911&tn=1#a14
[47] Artículo 8 del RGPD - Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información

información proporcionada por la Administración a través de su cuenta oficial y cuya legitimación para ser tratados por la AA.PP. estaría basada en el cumplimiento de una misión realizada en interés público o en el ejercicio de los poderes públicos conferidos.

Además, de cara a las responsabilidades asumidas por la AA.PP., y relacionado con las tecnologías de seguimiento (cookies) vistas en el punto previo de este documento, el tratamiento de datos realizado por la red social podría incurrir en la recogida de un volumen mayor de datos personales del ciudadano de los necesarios por parte de la Administración Pública en la gestión de su perfil oficial o de datos adicionales que no tengan ninguna relación con dicha gestión. El rol que la Administración Pública y la red social desempeñan respecto al tratamiento de los datos personales recogidos podría cambiar a corresponsables dependiendo de si la Administración Pública no es diligente para conocer dicha circunstancia, o, conociéndolos, tiene opciones para configurar o limitar el tratamiento que realiza la red social y no hace uso de ellos, o permite activamente que se produzca el tratamiento[48]. Por ejemplo, en caso de los widgets a las redes sociales incluidas en los portales de las AA.PP., antes de permitir el uso de cookies por dichos recursos, es necesario que las AA.PP. recaben el consentimiento previo del visitante de sus páginas, manteniendo los widgets deshabilitados hasta su obtención. Las AA.PP., en cualquier circunstancia, han de garantizar que los datos tratados son los estrictamente necesarios para el cumplimiento de los fines legitimados, en cumplimiento del principio de minimización.

La mayoría de las redes sociales no ofrecen niveles de calidad de servicio lo suficientemente contrastados para que se puedan convertir en instrumentos de notificación, ya que no se puede garantizar la integridad de la información proporcionada y que esta no va a ser recortada o enriquecida con publicidad u otros contenidos ajenos. Tampoco existen garantías de confidencialidad en la transmisión de una información a la red social ya que, en algunas de ellas, es posible el acceso al contenido por parte de la propia red social[49], o bien la configuración de privacidad del perfil del usuario puede permitir el acceso indiscriminado a las publicaciones realizadas, consentimiento que no es implícito sobre el contenido remitido por una Administración.

Normalmente, la entidad ha de disponer de una política de comunicación en redes sociales que ha de reflejar aspectos de la Política de Protección de Datos[50] de la entidad como son:

- Una responsabilidad clara y embebida de forma eficiente en la cadena de responsabilidades de la organización, de manera que la comunicación por la red o redes sociales esté bien alineada con el resto de la política de comunicación institucional.
- Un documento informativo para los empleados públicos donde se indique qué pueden hacer y qué no en la red social de la Administración. Si se parte de la base de que las redes sociales son un apoyo o complemento a una página web y una sede oficial, es más fácil limitar el servicio y evitar riesgos.
- Una formación adecuada a las personas encargadas de publicar contenidos y atender a comentarios y cuestiones, detallando:

[48] De acuerdo con lo establecido por el CEPD en su documento Directrices 07/2020 en relación con el concepto de responsable y encargado en el RGPD (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf) y en la sentencia del Tribunal de Justicia de la Unión Europea Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, 5 June 2018, pueden suponer una corresponsabilidad en el tratamiento de los datos recogidos. Sin embargo, esta última sentencia establece que el hecho de hacer uso de una red social no implica que se establezca la figura de corresponsabilidad, sino cuando se participa en la determinación del propósito y de los medios del tratamiento.

[49] Algunas redes sociales acceden a los contenidos para perfilar al usuario con propósitos de marketing. Otras para aplicar políticas contra la pederastia, violencia digital, análisis psicológico, etc., que pueden suponer una intrusión a su privacidad en el caso de mal interpretar comunicaciones oficiales.

[50] Artículo 24 del RGPD – Responsabilidad del responsable del tratamiento

- Qué información personal se puede publicar y cual no.
- En el caso de que se publiquen documentos extractados o anonimizados, debe hacerse con garantías para no divulgar, por ejemplo, los datos de la firma electrónica del firmante o el código seguro de verificación[51] que permitiría recuperar todo el documento.
- La forma en la que se debería dialogar con los usuarios.
- Cómo deben escalarse o comunicarse internamente los mensajes, avisos recibidos a través del canal que contengan datos de carácter personal y que precisen de atención, como solicitudes de retirada de contenidos, peticiones que revelan los datos del peticionario a terceros o incluso amenazas terroristas o mensajes de suicidas.

Las redes sociales pueden ser un medio para que las Administraciones conozcan datos estadísticos[52] de sus usuarios, a través de la información que proporciona la propia plataforma. Esto podría realizar un perfilado de los usuarios, de sus intereses y de sus tendencias de navegación. En la medida en la que involucran tratamientos de datos personales, además de estar legitimado, especialmente cuando de la navegación se pueden inferir categorías especiales de datos, se debe proporcionar información de dichos tratamientos de conformidad con los artículos 13 y 14 del RGPD.

Hay que tener presente que algunas redes sociales permiten reenviar contenido a terceros. En el caso de que pueda existir contenido con datos personales, hay que atender a lo que se manifiesta en el Considerando 66 del RGPD: *A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales*.

Buscar un posicionamiento o una influencia, como se podría realizar en otros ámbitos, acudiendo incluso a técnicas ilícitas como la compra de seguidores[53], la publicación de opiniones falsas o el abuso de las etiquetas y términos más buscados, podría interpretarse como una falta de transparencia y licitud con relación al tratamiento que se sustente en la utilización de una red social sin perder de vista la ausencia de calidad de datos[54] vinculada al incumplimiento del principio de exactitud .

C. RIESGOS PARA LOS DERECHOS Y LIBERTADES ASOCIADOS A LAS REDES SOCIALES DE LAS ADMINISTRACIONES

Una vez que se ha diseñado un tratamiento a través de redes sociales que cumple con los requisitos establecidos en el RGPD, es necesario analizar los riesgos que para los derechos y libertades de los ciudadanos se pueden originar, con el fin de llevar a cabo la gestión adecuada de los mismos.

Uno de los riesgos es que se produzcan errores en la aplicación de las políticas de comunicación a través de redes sociales que desvelen datos de carácter personal de forma

[51] Código seguro de verificación en el Gobierno de España: https://sede.administracion.gob.es/PAG_Sede/ayuda/ayudaCSV.html
[52] Por ejemplo, Facebook ofrece estadísticas para las páginas profesionales o *fan pages,* a diferencia de los perfiles o páginas personales. (https://es-la.facebook.com/business/insights/tools/audience-insights)
[53] Artículo sobre la compra de seguidores falsos en redes sociales https://www.genbeta.com/redes-sociales-y-comunidades/hemos-comprado-seguidores-falsos-twitter-instagram-facebook-se-nos-ha-quedado-cara-tonto
[54] Artículo 5.1.d) del RGPD – Principios relativos al tratamiento. Principio de exactitud

indeseada tanto de los administrados como de los propios empleados públicos (publicación de CSV[55], metadatos, ...). Para reducir el riesgo es necesaria la definición de una política interna clara y bien conocida por el personal sobre las implicaciones y consecuencias de la participación en redes sociales.

En esa política se deben definir tanto las directrices de la gestión de las cuentas oficiales, de las redes internas, así como los consejos para la participación, a título personal, en redes no oficiales. En particular, debe detallarse aquello que puede publicarse o no en redes sociales[56], las consecuencias para aquellos que vulneren las normas, las actividades de formación que han de seguir los empleados, la auditoría periódica de los procesos de publicación, así como una vigilancia permanente, por parte de las personas de la organización que gestionan la presencia en las redes, para velar por la seguridad de los tratamientos[57] realizados en este contexto y dar una respuesta proactiva a cualquier incidencia[58].

Por ejemplo, en la difusión de contenido por parte de las AA.PP. a través de servicios de mensajería instantánea, la utilización de listas de difusión o canales, en lugar de grupos, evita la identificación de los participantes entre sí.

También es aconsejable, además de los cursos de formación impartidos entre el personal involucrado, comprobar periódicamente que se cumplen las políticas definidas por la entidad con relación a las redes sociales internas, el uso del BYOD o la utilización de redes personales en las que se divulga información personal relativa a la entidad.

Entre los elementos que hay que comprobar y de los que hay que hacer un seguimiento continuo, destacan:

- Datos personales de empleados de la Administración: ¿los publicadores lo hacen con su nombre, o se publican datos de DNI completos[59], nóminas o patrimonio de altos cargos directamente en la red?[60] ¿Se publican fotografías de las oficinas o de eventos internos sin tomar las medidas adecuadas?
- Expedientes o casos tramitados por la Administración: ¿Se publican ejemplos o resoluciones completas mal anonimizadas, o se proporciona información del estado de tramitación a personas que dicen ser interesados sin realizar ningún tipo de comprobación previa?
- Aspirantes a empleados o alumnos de cursos de formación: ¿Se publican listas, notas, o fotografías de cursos tomadas sin las debidas precauciones?
- Usuarios de la red social: ¿Se revelan datos de su identidad en los comentarios?
- Datos inferidos que pudieran deducirse relativos a una persona física determinada como resultado de una publicación.

Herramientas para realizar esta comprobación pueden ser, por ejemplo, revisión periódica de contenidos manual o automática, encuestas entre los empleados o auditorías periódicas.

---

[55] https://www.rtve.es/noticias/20181018/cgpj-atribuye-fallo-sistemico-filtracion-datos-victima-manada/1822280.shtml

[56] El término más preciso es una Social Media Policy. https://www.forbes.com/sites/forbeshumanresourcescouncil/2017/05/25/why-your-business-needs-a-social-media-policy-and-eight-things-it-should-cover/#3f09e7495264

[57] Artículo 32 del RGPD – Seguridad del tratamiento

[58] La AEPD tiene un documento específico sobre consecuencias administrativas, disciplinarias, civiles y penales de la difusión de contenidos sensibles en https://www.aepd.es/sites/default/files/2019-12/consecuencias-administrativas-disciplinarias-civiles-penales.pdf

[59] La AEPD publicó en 2019 una orientación para la aplicación provisional de la Disposición adicional séptima de la LOPDGDD. https://www.aepd.es/sites/default/files/2019-09/orientaciones-da7.pdf

[60] En la publicación de información pública ha de estarse a los criterios interpretativos conjuntos emitidos por la Agencia Española de Protección de Datos y el Consejo de Transparencia y Buen Gobierno sobre el alcance de los órganos, organismos y entidades del sector público estatal en materia de acceso a la información pública sobre sus Relaciones de Puestos de Trabajo (RPT), catálogos, Plantillas orgánicas, etc. y las retribuciones de sus empleados públicos o funcionarios (CI/001/2015) y el personal eventual en la Administración General del Estado y la aplicación del art. 19.3 de la Ley de Transparencia (CI/001/2020)

Con relación a la publicación de información anonimizada, como se ha señalado anteriormente, el contenido anonimizado publicado ha de ser sometido a revisión tanto de forma automática como manual para garantizar de que no se ha producido un error en el proceso de anonimización que exponga datos personales de los administrados o empleados públicos. Hay que incluir procedimientos para revisar los metadatos que puedan estar incluidos en la documentación publicada, tanto los que revelen información de los empleados públicos como otros datos que permitan acceder a la información original de documentos anonimizados, como los CSVs.

En los procesos de anonimización del contenido que se va a publicar en la red social, es aconsejable tener una compartimentación clara entre aquel contenido anonimizado del no-anonimizado, así como otras garantías que dificulten la posibilidad de publicación por error de contenidos con datos de carácter personal. En particular, es recomendable evitar que el gestor de la red social tenga fácil acceso a contenido no anonimizado.

Atendiendo al principio de minimización, siempre que no sea necesario para el tratamiento la identificación del administrado se debe evitar recoger y tratar ese dato. Existe un riesgo de reidentificación y perfilado de los administrados a través del análisis de las visitas realizadas como de la consulta a contenidos específicos. Como en el caso de las cookies, hay servicios más sensibles, como de asesoría a menores o víctimas, consultas de salud, buzones anónimos de denuncia, etc., que pueden comprometer al propio usuario al registrarse hábitos de navegación, mostrar contenido a partir de perfilado contextual o la reidentificación antes señalada que generan riesgos que es necesario gestionar.

Por ejemplo, cuando se lleven a cabo procesos de participación o encuesta de los ciudadanos a través de la red social, hay que analizar los riesgos de reidentificación por terceros vinculados con los metadatos recogidos en el proceso de encuesta, como direcciones IP o firmas de los dispositivos empleados por los usuarios, así como la posible vinculación de las respuestas con otros datos de carácter personal en poder de la Administración Pública.

Las cuentas abiertas en una red social por una Administración Pública pueden verse comprometidas y por tanto se puede infiltrar contenido en ellas con el propósito de recabar datos de carácter personal. Esto tiene que ser tenido en cuenta a la hora de gestionar los procesos de asignación y renovación de claves de acceso.

Por otro lado, el contenido de terceros, insertado como anuncios o de otra forma, puede llevar a engaño a los usuarios y hacer creer a estos que son enlaces que pertenecen a servicios de la Administración Pública que recaban datos personales, por lo que dichos contenidos han de estar bajo supervisión o controlar el tipo de contenidos que se puede ofrecer, en particular, contenidos relacionados con ideologías y creencias de cualquier índole.

En el caso de que se proporcionen espacios a los administrados para subir sus propios contenidos, se recomienda evitar que la publicación de dichos contenidos se realice sin supervisión para evitar la divulgación de información personal de terceros sin su consentimiento, en particular, contenido sensible o cualquier conducta que tuviera implícitos actos de violencia digital.

En caso de que acceso a los contenidos de la red social requieran iniciar una sesión por parte del administrado, la Administración Pública ha de evaluar las garantías de privacidad, incluyendo las medidas de seguridad orientadas a la privacidad que proporciona dicha red, especialmente la política de creación de usuarios y contraseñas. Este análisis ha de

realizarse en interés de los ciudadanos, pero también en la de los gestores del espacio pudiendo un atacante suplantar a los publicadores[61].

Además, de cara a las responsabilidades asumidas por las AA.PP. y relacionado con las tecnologías de seguimiento vistas en el punto previo de este documento, es preferible que en el sitio web de la Administración, o en las *newsletters* que se distribuyan, se incluyan enlaces estáticos al perfil oficial en la red social, frente al empleo de *widgets* embebidos en el contenido.

En ese caso, las AA.PP. tienen la obligación de comprobar que dicho enlace conduce a los ciudadanos a un servicio de Internet que cumple con los establecido en la normativa. Por ejemplo, si dicho sitio web utiliza cookies de las que es necesario informar y recabar el consentimiento previo para tratamientos como perfilado y tracking, es necesario que exista una comprobación periódica que dicha circunstancia se cumple de forma efectiva.

Finalmente, aunque se han señalado anteriormente las obligaciones de cumplimiento con relación a los menores, hay que ser consciente de que las técnicas actuales no siempre permiten determinar con total efectividad que el usuario pueda ser un menor de edad. Habrá que evaluar el riesgo que esto supone con relación al tipo de contenidos que se están ofreciendo a través de la red y, en función de este riesgo, establecer procedimientos adicionales para la comprobación más precisa de la edad de los usuarios.

[61] En el blog de la AEPD hay un post dedicado a las Medidas de seguridad en Facebook (https://www.aepd.es/es/prensa-y-comunicacion/blog/medidas-de-seguridad-en-facebook)

IV. CLOUD COMPUTING O COMPUTACIÓN EN LA NUBE

A. QUÉ ES LA COMPUTACIÓN EN LA NUBE

La computación en la nube o *cloud computing*[62] es una forma de usar los servidores en localizaciones remotas de una forma flexible y transparente. En lugar de contar con equipos propios, comprados y alojados en las instalaciones de la organización, un proveedor 'alquila' equipos virtuales o servicios específicos, que se gestionan a través de la red. Este modelo elimina los problemas de las inversiones iniciales y la obsolescencia, permitiendo al cliente que en cada momento pague por la capacidad de cómputo, el ancho de banda o los servicios que necesita. El prestador del servicio puede garantizar por contrato los parámetros de calidad de servicio, las garantías de privacidad, de seguridad orientada a otros propósitos, mantenimientos, actualización de los paquetes software, etc.

Aunque en los primeros tiempos de la computación en la nube las herramientas ofrecidas por el proveedor eran iguales a los que podía comprar un cliente y alojar en sus máquinas, en la actualidad existen bases de datos, bibliotecas, lenguajes de programación y componentes software específicos para la nube[63], así como certificaciones[64], especialistas y toda una disciplina académica[65].

Atendiendo al tipo de servicios ofrecidos al cliente, podemos distinguir entre soluciones IaaS (Infraestructura como Servicio) si el proveedor sólo proporciona capacidad de almacenamiento y proceso en bruto; PaaS (Plataforma como servicio), si se proporcionan las utilidades básicas para construir aplicaciones sobre las que desarrollar soluciones, y SaaS (Software como servicio) cuando el cliente encuentra en la nube todas las herramientas finales para implementar los procesos de su organización. Otra posible clasificación de las nubes es la separación entre públicas y privadas. Hablamos de nube pública cuando los proveedores proporcionan servicios 'sueltos' a diferentes clientes, como espacio para webs, almacenamiento o capacidad de proceso. En el otro extremo, hablamos de nube privada cuando el proveedor ofrece una serie de servicios agrupados y de forma cerrada a terceros. Podríamos comparar una nube privada con una red privada o una intranet de una organización, con sus elementos aislados del exterior, salvo por accesos localizados, y con una gestión centralizada.

Con la popularización de los servicios en la nube en ocasiones se ofrecieron servicios que no eran transparentes sobre la ubicación donde se procesan los datos[66]. Esta virtualización y deslocalización no está exenta de riesgos tanto para la seguridad como la protección de los datos personales[67].

B. LA COMPUTACIÓN EN LA NUBE Y LAS AA.PP.

Las AA.PP. usan la nube como parte de los servicios prestados a los ciudadanos y como elemento de su gestión interna. De hecho, la Secretaría General de Administración Digital proporciona a la Administración General del Estado y sus organismos públicos un servicio

[62] Wikipedia https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube
[63] Amazon web Services tiene hasta 21 categorías de productos específicos para su nube. https://aws.amazon.com/es/products/
[64] Las más populares son las de AWS, CISCO, Microsoft y WMWARE
[65] Google Scholar devuelve 6310 papers sobre Cloud computing solo en 2020. https://scholar.google.es/scholar?as_ylo=2020&q=academic+papers+cloud+computing&hl=es&as_sdt=0,5&as_vis=1
[66] Regiones de Azure https://azure.microsoft.com/es-es/global-infrastructure/regions/
[67] La AEPD tiene publicada una Guía para clientes que contraten servicios de Cloud Computing (https://www.aepd.es/sites/default/files/2019-09/guia-cloud-clientes.pdf) y unas Orientaciones para prestadores de servicios de Cloud Computing (https://www.aepd.es/sites/default/files/2019-09/guia-cloud-prestadores.pdf).

de computación y almacenamiento en modo nube híbrida a través del servicio compartido Nube SARA[68].

Los servicios en la nube facilitan que las Administraciones puedan contar con un catálogo de servicios 'marca blanca', y adaptarlos y desplegarlos[69] sin una inversión en activos, optando por un modelo de gobernanza muy flexible y escalable, lo que podría resultar interesante en el caso de Administraciones pequeñas con pocos recursos, como Diputaciones o Entidades Locales. Para que esta facilidad no se convierta en un problema es necesario planificar con cuidado, al menos desde el punto de vista del cumplimiento de la normativa de protección de datos, la forma de implementar los servicios y con qué *partners* se van a implementar.

Además, la nube no permite un control directo sobre los servicios, y cuando se producen errores, brechas o discontinuidad del servicio, se depende del conocimiento de terceros externos y de unos tiempos de respuesta regulados por acuerdos de nivel de servicio (SLA, o *service level agreement*[70]), establecidos por contrato. Cuando se opta por contratar servicios en la nube es obligación de responsable del tratamiento el asegurarse que selecciona el proveedor adecuado[71] además de garantizar que dicho contrato contiene las cláusulas y garantías necesarias que comprometen al proveedor de servicios en el cumplimiento de la norma de protección de datos, así como el resto de normativa que fuera de aplicación a una determinada entidad pública. En todo caso, es importante tener en cuenta que la información publicitaria o los documentos técnicos descriptivos publicados en la página web del proveedor sobre los servicios en la nube ofrecidos no suponen, por si mismos, condiciones contractuales y vinculantes respecto de la prestación de un servicio, salvo que se incorporen a la oferta suscrita con el prestador adjudicatario de la licitación. En ningún caso, un contrato de adhesión genérica a un determinado servicio puede entenderse como vinculante cuando se establecen condiciones al margen de los requisitos generales de contratación para las Administraciones Públicas que determina la Ley de Contratos del Sector Público[72].

Muchas veces se tiende a identificar la nube con la nube pública, más barata y popular, dejando a un lado la posibilidad de configurar y compartir nubes privadas para una Administración o un conjunto de éstas. Existen proveedores que ofrecen nubes privadas con certificaciones de seguridad, permitiendo así ofrecer a sus clientes no solo una facilidad en el desarrollo de sus servicios, sino también en la certificación de seguridad de sus Administraciones.

La contratación de un servicio en la nube no supone el desplazamiento total de las obligaciones de gestión de la seguridad al encargado del tratamiento sino que corresponde

---

[68] De acuerdo al Catálogo de servicios de Administración digital publicado en el Portal Administración electrónica, Nube SARA forma parte de los servicios declarados como compartidos (CETIC 15/09/2015) y proporciona servicios de computación y almacenamiento en nube híbrida para la AGE y sus Organismos Públicos, mediante la configuración de nodos de consolidación tanto en CPDs de la Administración (nube privada) como de proveedores externos (nube pública) lo que permite a las unidades TICs clientes del servicio proveerse de capacidades tanto en nube privada como en nube pública para cada uno de los servicios que tengan que implantar atendiendo a sus características y los costes que puedan asumir. Aunque inicialmente se centra en la infraestructura como servicio, la idea es proporcionar gradualmente servicios de mayor madurez, tales como plataforma como servicio y aplicación como servicio (por ejemplo, gestión de la nómina en la nube). Los componentes del servicio prestados serán los habituales en servicios de estas características: provisión de servidores virtuales con diferentes características configurables, almacenamiento compartido, comunicaciones, backup, alta disponibilidad de componentes, monitorización, control del consumo, …

[69] Existen diversas tecnologías que facilitan el despliegue de instancias de servicios rápidamente, de una forma más ligera que las máquinas virtuales. El lector interesado puede leer, por ejemplo, sobre Docker (https://www.docker.com/resources/what-container) o Kubernetes (https://kubernetes.io/es/docs/concepts/overview/what-is-kubernetes/)

[70] Acuerdo de nivel de servicio en la Wikipedia https://es.wikipedia.org/wiki/Acuerdo_de_nivel_de_servicio

[71] Artículo 28.1 RGPD: *"Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado."*

[72] https://www.boe.es/buscar/act.php?id=BOE-A-2017-12902

siempre al responsable de un tratamiento la toma de decisiones con relación a los requisitos de protección de datos personales entre los que, necesariamente, se deberá de contar con los requisitos de seguridad que establece el artículo 32 del RGPD.. A parte de las obligaciones de supervisión que tiene el responsable sobre las medidas a cargo del encargado, el responsable siempre tendrá la obligación de implementar alguna de esas medidas, como podría ser, la definición y gestión de la política de control de accesos.

Otra obligación de la Administración Pública es la de solicitar y obtener información sobre si intervienen o no terceras personas (subcontratistas) en la prestación de servicios de *cloud computing* y ejecutar el control de las mismas tal como se describe en la Guía para clientes que contraten servicios de Cloud Computing[73]. Además, debe quedar claro en el contrato de la nube dónde se ubican físicamente los servidores que van a albergar los datos personales. Si los servidores se encuentran en otro país debemos asegurarnos de que mantiene unas garantías equivalentes[74] en protección de datos personales.

Existe otra restricción respecto de la ubicación de los servidores del proveedor de servicios de *cloud computing* contratado introducida por el Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de Administración Digital, contratación del sector público y telecomunicaciones[75]. Esta norma, mediante la modificación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público[76], establece la obligación de que la empresa adjudicataria presente, antes de la formalización del contrato, una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos. Esta información puede ser importante para los intereses de la seguridad nacional. También es necesario asegurar el sometimiento de la ejecución de ese contrato a la normativa nacional y de la Unión Europea en materia de protección de datos.

La Administración Pública deberá tener en cuenta los requisitos de protección de datos a lo largo de todo el ciclo de vida de prestación del servicio, no solo desde el momento de la elección del proveedor del servicio o durante la prestación del servicio en sí misma, sino que, una vez concluida la relación contractual, ha de asegurar que la información se destruya, se devuelva a la entidad contratante o se traspase a un nuevo encargado del tratamiento que haya sido designado, para lo que necesariamente deberá tenerse en cuenta lo establecido en el Esquema Nacional de Interoperabilidad[77]. Con este fin, y al objeto de asegurar el cumplimiento normativo, es recomendable realizar auditorías y requerir certificaciones de cumplimiento periódicas.

C. RIESGOS PARA LOS DERECHOS Y LIBERTADES ASOCIADOS A LA COMPUTACIÓN EN LA NUBE

A pesar de las ventajas que aporta la nube, este tipo de soluciones presentan también una serie de riesgos que deben ser tenidos en cuenta. Entre ellos estarían la privacidad de la información almacenada, así como la continuidad de los servicios, los cambios legales y la pérdida de control de la infraestructura y de las aplicaciones utilizadas. En el caso particular de las AA.PP., por el volumen y la sensibilidad de los datos que gestionan, estos riesgos deben ser objeto de un riguroso análisis en cada escenario en que se plantee la

[73] Detalladas en el capítulo "Lo que debo conocer para la contratación de Servicios de Cloud Computing", en particular en su apartado 4.
[74] Artículo 44 del RGPD – Principio general de las transferencias
[75] BOE núm. 266, de 5 de noviembre de 2019 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2019-15790
[76] Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. https://www.boe.es/buscar/act.php?id=BOE-A-2017-12902
[77] https://www.boe.es/buscar/act.php?id=BOE-A-2010-1331

utilización de este tipo de soluciones, en particular, cuando de los servicios desplegados en la nube dependan los derechos y libertades de los ciudadanos.

Igualmente, es también importante evaluar qué tipo de arquitectura *cloud*, pública o privada, representa un menor nivel de riesgo para el tratamiento específico que se desea implementar. No debe perderse de vista que la no posibilidad de cumplir técnicamente con alguna de las obligaciones exigidas por el RGPD al responsable no debe ser considerada un riesgo susceptible de tratar sino un incumplimiento normativo. En ningún caso, los requisitos de cumplimiento del RGPD y la LOPDGDD pueden reemplazarse con medidas técnicas y organizativas.

A la hora de diseñar el tratamiento, es conveniente evaluar la incorporación y aplicación de mecanismos de minimización de datos en función del riesgo, en particular, limitar la extensión de los datos[78], subir a la nube datos anonimizados o seudonimizados, emplear cifrado homomórfico[79], etc.

Los datos de los empleados públicos también pueden estar expuestos. Hay que evaluar el riesgo de que información de los empleados, sobre todo cuando están teletrabajando y/o utilizando BYOD, pueda estar expuesta a terceras partes, en particular metadatos que expongan su vida privada. El contexto en el que puedan ubicarse las actividades laborales de los empleados públicos no exime, en ningún caso, la responsabilidad de las Administraciones Públicas con relación a la normativa de protección de datos.

A la hora de identificar la información que se sube a la nube, muchas veces surge la duda de si realmente se corresponde con datos personales y cumplen con el principio de minimización[80]. Puede tratarse de datos agregados, comprimidos o sobre los que se ha aplicado alguna técnica para desvincularlos de las personas físicas, pero no por ello tienen que dejar de ser datos personales si tras ellos, hay personas que, con alguna posibilidad, podrían ser identificables. Es una cuestión que hay que analizar formalmente y evaluar con rigor y seriedad los riesgos de reidentificación, evitando las respuestas simplistas con el propósito de eludir la responsabilidad de tratar datos personales. Esta aproximación ha de formar parte de otra más integral que evalúe el nivel de madurez de los procesos de anonimización[81] utilizados por la organización.

Durante la vida del sistema es importante que se monitorice adecuadamente su funcionamiento y se audite la implementación del servicio, que evolucionará en el tiempo. Esta actitud proactiva es, en primer lugar, una responsabilidad[82] de los 'responsables' del servicio, pero estos deben extenderla por toda la cadena de encargos y subcontrataciones. En caso de una infracción de la normativa de protección de datos, el responsable no puede escudarse en que no sabía lo que hacían sus encargados pues, como ya se ha indicado, de acuerdo a artículo 28 del RGPD, este es responsable tanto de elegir a un encargado que ofrezca garantías como de estipular formalmente, a través de un contrato, las instrucciones y el modo de proceder del encargado cuando realice el tratamiento de los datos personales.

No es improbable que en los servicios en la nube se produzcan brechas de seguridad que pongan en peligro la disponibilidad, la integridad o la confidencialidad de los datos

[78] Considerando 78 y artículo 25 RGPD.

[79] El cifrado homomórfico es una técnica que permite realizar operaciones sobre los datos cifrados y obtener resultados, también cifrados, equivalentes a las operaciones realizadas directamente sobre la información original. En el post Cifrado y Privacidad III: Cifrado Homomórfico (https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-privacidad-iii-cifrado-homomorfico) publicado por la Agencia Española de Protección de Datos puede ampliarse la información sobre esta técnica de minimización de datos.

[80] Artículo 5.1.c) del RGPD – Principios relativos al tratamiento. Principio de minimización

[81] Privacy Analytics, "The De-identification Maturity Model", Khaled El Emam, PhD, Waël Hassan, PhD. 2013 https://iapp.org/media/pdf/resource_center/2014-14-05%20Privacy%20Analytics%20The%20De-identification%20Maturity%20Model.pdf

[82] Artículo 5.2 del RGPD – Principios relativos al tratamiento. Responsabilidad proactiva

personales con consecuencias para los derechos y libertades de las personas físicas. Un ciberataque, un malfuncionamiento del sistema o un error humano pueden poner en peligro los datos de los ciudadanos y de los empleados públicos. Como se ha indicado antes, la gestión del riesgo de seguridad de la información no recae de forma exclusiva en el proveedor del servicio, sino que corresponde al responsable determinar las medidas de seguridad que debe de exigir al encargado y que, obligatoriamente, han de quedar reflejadas de forma contractual.

Con relación a este último punto, en el caso de producirse una brecha de seguridad que afecte a datos personales, el responsable tiene que poner en marcha una serie de mecanismos de forma urgente[83]. Por un lado, debe hacer frente a la propia contingencia de la manera que considere menos arriesgada para los datos y el servicio en general. Paralelamente, y en un plazo de 72 horas debe notificar a la Autoridad de Protección de Datos la información que tiene de la quiebra[84] . No es solo un trámite estadístico o burocrático, sino que tiene como objeto crear una sociedad más resiliente, al permitir a la Autoridad de Control y a otras entidades, ganar conocimiento respecto a la materialización de ciertos riesgos y así poder reaccionar proactivamente. Asimismo, en determinadas situaciones, la Autoridad de Control puede ordenar al responsable que comunique a los usuarios[85] cuyos datos se han visto afectados por la brecha de seguridad que se ha producido esta, para que permanezcan alerta o adopten sus propias medidas de seguridad y protección frente al incidente.

La Administración, como responsable del tratamiento, también ha de gestionar los riesgos en el caso de que el proveedor de la nube decida, de forma unilateral, discontinuar el servicio o cambiar las condiciones en que se presta, así como gestionar el riesgo legal de que existan cambios normativos o de otra naturaleza que impidan la utilización de dichos servicios. Esto último es particularmente importante en aquellos proveedores que no están localizados en el territorio nacional, por lo que el responsable, en respuesta a un análisis de los posibles riesgos[86], ha de desarrollar las medidas necesarias y tener implementados planes de contingencia y estrategias de migración de los servicios a otros sistemas.

[83] La AEPD ha publicado una Guía para la gestión y notificación de brechas de seguridad. Está en https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf . También hay varios artículos en su blog (https://www.aepd.es/es/prensa-y-comunicacion/blog) sobre este tema. El WP29 también publicó unas directrices en febrero de 2018 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052)

[84] Artículo 33 del RGPD – Notificación de la violación de la seguridad de los datos personales a la autoridad de control

[85] Artículo 34 del RGPD – Comunicación de una violación de seguridad de los datos personales al interesado

[86] Artículo 32 del RGPD – Seguridad del tratamiento

V. BIG DATA O TRATAMIENTO MASIVO DE DATOS

A. QUÉ ES EL BIG DATA

De acuerdo con la definición dada por ISO, cuando hablamos de *Big Data*[87], o tratamiento masivo de datos, nos referimos a grandes conjuntos de datos, caracterizados por su volumen, variedad, velocidad y/o variabilidad, que requieren de una tecnología escalable para un almacenamiento, manipulación, gestión y análisis eficiente.

Las tecnologías de tratamiento masivo se han desarrollado mucho en los últimos años abriendo un amplio abanico de tratamientos. Internet ha puesto a disposición de todos nosotros una gran cantidad de datos que pueden ser utilizados. Las propias AA.PP., a través de la Iniciativa Aporta[88] y el portal datos.gob.es, promovido por el Ministerio de Asuntos Económicos y Transformación Digital y la Entidad Pública Empresarial Red.es, promociona la apertura y reutilización de la información pública y el desarrollo de servicios avanzados basados en datos.

El análisis masivo de datos nos ha permitido obtener informaciones en tiempo real, o casi real, a partir de fuentes de información y conjuntos de datos repartidos por todo el mundo. Existen plataformas software específicas para extraer, cargar y transformar (se emplean las siglas ELT o *Extract, Load and Transform* frente al acrónimo ETL de los cuadros de mando) datos de distintos orígenes y explotar esa información. Esta explotación puede tomar formas muy variadas, que irían desde presentarla de una forma gráfica, por ejemplo, como cuadros de mando, a construir nuevas informaciones o perfiles, reagrupando los datos de una forma distinta a como se han obtenido.

Desde el punto de vista de la protección de datos personales es capital asegurarse que existe una legitimación[89] para dicho tratamiento masivo de datos y, en el caso de que se incluyan categorías especiales de datos, es necesario levantar previamente la prohibición para su tratamiento[90] . Estas condiciones no sólo han de cumplirse para los datos incluidos en la colección de datos recogidos sino también para aquellos que puedan ser inferidos a partir del cruce y conexión de los datos originales.

En la fase de diseño de los tratamientos de *Big Data* hay que analizar de forma objetiva qué cantidad de datos es necesaria y suficiente con relación al objetivo del tratamiento[91], ajustarse al principio de minimización de datos[92] y no adoptar estrategias de "por si acaso" en las que, sin haber establecido criterios de selección previos, se recurre a recoger la máxima cantidad posible de datos. Este problema se puede ver acentuado en el caso de recopilación masiva de datos soportada por sensores en contextos de tratamiento como los realizados en las *Smart Cities*.

Esta tecnología permite el perfilado o el enriquecimiento de perfiles de personas, tratamiento que precisa de una legitimación y debe cumplir unos requisitos y condiciones, entre ellas las relativas a las decisiones individuales automatizadas[93], y en su caso, la

[87] ISO/IEC 20546:2019 Tecnología de la información – Big Data – Resumen y vocabulario

[88] La Iniciativa Aporta https://datos.gob.es/sites/default/files/datosgobes/190522_iniciativa_aporta_-_contexto_y_directrices.pdf se desarrolla en el contexto del marco legislativo vigente https://datos.gob.es/sites/default/files/datosgobes/190522_iniciativa_aporta_-_contexto_y_directrices.pdf y se articula la plataforma datos.gob.es como punto de encuentro entre las Administraciones, las empresas y los ciudadanos que forman parte del ecosistema de los datos abiertos en España.

[89] Artículo 6 del RGPD – Licitud del tratamiento

[90] Artículo 9 del RGPD – Tratamiento de categorías especiales de datos personales https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e2114-1-1

[91] Con relación a la aplicación del principio de minimización, consultar la Guía de Protección de Datos por Defecto de la AEPD.

[92] Artículo 5.1.c) del RGPD – Principios relativos al tratamiento. Principio de minimización

[93] Artículo 22 del RGPD - Decisiones individuales automatizadas, incluida la elaboración de perfiles

realización de una evaluación de impacto para la protección de datos[94] y si procede, la consulta previa[95] a la Autoridad de Control.

Si se han inferido datos personales, debemos manejarlos como datos personales, con todas las garantías en cuanto a seguridad[96], derechos[97], transferencias internacionales[98] y otros.

Si el mismo responsable del tratamiento masivo de datos ha sido el que ha recogido la información personal directamente de los interesados[99], por ejemplo a través de apps, formularios en internet o usando *cookies* u otras tecnologías, debe preocuparse de que puede hacerlo, y en el caso de que esa legitimación[100] la proporcione el consentimiento de los usuarios, que éste sea recogido de manera apropiada[101] y la transparencia de la información[97] sea máxima de modo que los usuarios sean plenamente conscientes de dónde, cómo y para qué se van a usar sus datos y los mecanismos existentes para reclamar sus derechos sobre ellos o retirar el consentimiento prestado. En caso de que no se hayan recogido los datos personales directamente por el responsable que realiza el tratamiento, hay que tener en cuenta las obligaciones y los requisitos de información que también establece la normativa[102].

Si el tratamiento se hace por cuenta de un tercero que actúa como encargado[103], como se ha visto en otra tecnologías de las ya analizadas, es preciso formalizar un contrato detallando cómo se van a tratar los datos desde su puesta a disposición hasta que se devuelvan o se destruyan, incluyendo las medidas de seguridad y las garantías adicionales que deben adoptarse.

B. BIG DATA Y LAS AA.PP.

El *Big Data*, en conjunción con otras tecnologías señaladas en este documento, como por ejemplo la computación en la nube o la inteligencia artificial, es una herramienta que permite procesar y extraer valor de los grandes volúmenes de información que generan las AA.PP.

Por un lado, las Administraciones liberan muchos datos en formatos sencillos dentro de las iniciativas de datos abiertos[104]. Estas iniciativas, cada vez más extendidas, consideran la apertura de datos como una forma de transparencia[105] y pretenden hacer accesibles y reutilizables los datos referentes a población, transporte, entorno, salud, energía, territorio, educación, etc., que las AA.PP. tienen almacenados en sus sistemas. El propósito es facilitar información a los ciudadanos en un ejercicio de transparencia que ayude a generar mayor confianza en el organismo, y también al sector empresarial para que integre estos datos en sus sistemas y los aproveche en sus propios procesos, contribuyendo así al fomento de la economía y la innovación.

---

[94] Artículo 35 del RGPD – Evaluación de impacto relativa a la protección de datos
[95] Artículo 36 del RGPD – Consulta previa
[96] Artículo 32 del RGPD – Seguridad del tratamiento
[97] Artículo 12 del RGPD - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado
[98] Artículo 44 del RGPD – Principio general de las transferencias
[99] Artículo 13 del RGPD - Información que deberá facilitarse cuando los datos personales se obtengan del interesado
[100] Artículo 6 del RGPD – Licitud del tratamiento
[101] Artículo 7 del RGPD – Condiciones para el consentimiento
[102] Artículo 14 del RGPD - Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado
[103] Artículo 28 del RGPD – Encargado del tratamiento
[104] Iniciativa de Datos Abiertos del Gobierno de España https://datos.gob.es/
[105] En Europa partimos de la Directiva 2003/98/CE, de 17 de noviembre de 2003, actualizada por la Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio. En España han dado lugar a la Ley 37/2007, de 16 de noviembre, de reutilización de la información del sector público, actualizada por la Ley 18/2015, de 9 de julio. Hay más información normativa en https://datos.gob.es/sites/default/files/datosgobes/190522_iniciativa_aporta_-_contexto_y_directrices.pdf

Por otra parte, aquellas Administraciones con capacidad para analizar esos grandes conjuntos de datos han desarrollado equipos y están cruzando diferentes fuentes de información para extraer conocimiento y aplicar ese gran potencial que supone el análisis masivo de datos en diferentes sectores y escenarios como el sanitario, el turístico, la investigación, el desarrollo sostenible, la seguridad o la lucha contra el fraude.

Sin embargo, no debe perderse de vista que este análisis masivo y cruce de fuentes de fuentes de información heterogénea también puede tener consecuencias negativas desde el punto de vista ético, de la privacidad y, en particular, en la protección de datos, si se hace un mal uso de la información obtenida.

Como en todo tratamiento, se ha de cumplir el principio de licitud, lealtad[106] y limitación del tratamiento[107]. En el caso de los tratamientos basados en *Big Data*, por su propia naturaleza, parece relativamente fácil derivar en situaciones en las que la finalidad inicial del tratamiento se vea difuminada cuando el dato es explotado con finalidades secundarias, pues la normativa de protección de datos no impide que los datos personales puedan reutilizarse para finalidades diferentes para las que fueron recogidos, si no que éstas no deben ser incompatibles con las iniciales. Por lo tanto, para su reutilización en nuevos proyectos, resulta clave realizar un análisis de no incompatibilidad en el que debe tenerse en cuenta las siguientes consideraciones recogidas en el artículo 6.4 y el Considerando 50 del RGPD:

- Qué exista una relación entre la finalidad inicial del tratamiento y otras finalidades posteriores.
- Que dichos tratamientos posteriores se encuentren dentro de las expectativas razonables de los interesados.
- La naturaleza y sensibilidad de los datos objeto de tratamiento.
- El impacto que el tratamiento posterior puede tener sobre los interesados.
- Que se hayan adoptado medidas de protección, técnicas y organizativas, adecuadas.

Es importante tener en cuenta que no todas las bases legitimadoras se pueden invocar para el caso de tratamientos realizados por las AA.PP., en particular, las limitaciones establecidas para invocar el interés legítimo.

C. RIESGOS PARA LOS DERECHOS Y LIBERTADES ASOCIADOS AL BIG DATA

El Reglamento General de Protección de Datos aborda el tema de los tratamientos a gran escala y requiere de ellos que se adopten precauciones especiales[108] ya que, desde el punto de vista de la protección de datos personales, el procesamiento de grandes volúmenes de información puede encerrar riesgos que es necesario gestionar[109]. El tratamiento masivo de datos de carácter personal es uno de los supuestos para los que el RGPD exige una evaluación del riesgo más sistemática, requiriendo la realización de una evaluación de impacto relativa a la protección de datos[110] y, en su caso, en función del resultado obtenido, de una consulta previa[111] a la Autoridad de Control.

[106] Artículo 5.1.a) del RGPD - Principios relativos al tratamiento. Principio de licitud, lealtad y transparencia
[107] Artículo 5.1.b) del RGPD - Principios relativos al tratamiento. Principio de limitación de la finalidad
[108] Los tratamientos a gran escala aparecen en el artículo 35 (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3596-1-19) y 37 (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3792-1-1) , y en los considerandos 80, 91 y 97. Puede haber tratamientos a gran escala que no se usen Big Data, y usos del Big Data que no implican tratamientos a gran escala.
[109] La AEPD publicó ya hace algunos años un Código de buenas prácticas en protección de datos para proyectos Big Data (https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf)
[110] Artículo 35 del RGPD - Evaluación de impacto relativa a la protección de datos
[111] Artículo 36 del RGPD – Consulta previa

En este sentido, es preciso tener en cuenta que el carácter masivo de un tratamiento o el tratamiento de datos a gran escala, no se define exclusivamente por la cantidad de datos o por el número de personas cuyos datos pudieran procesarse en un determinado momento, atendiendo a lo señalado en el documento del Grupo de Trabajo del Artículo 29 de la anterior Directiva sobre "Directrices sobre los delegados de protección de datos (DPD)", el término "a gran escala" que está asociado a los procesos de *Big Data* debe de entenderse en varias dimensiones:

- Con relación al número de interesados afectados
- Con relación al volumen o variedad de elementos de datos que son objeto de tratamiento
- Con relación a la duración o permanencia de la actividad de tratamiento de datos
- Y con relación al alcance geográfico del tratamiento de *Big Data*

Sin perjuicio de otras consideraciones que pudieran derivar del contexto específico de determinadas operaciones de tratamiento de datos como puede ser el caso de la frecuencia con la que determinadas operaciones de tratamiento puedan llevarse a cabo partiendo de los datos obtenidos inicialmente.

Así, al abordar el desarrollo de una solución basada en *Big Data*, la Administración responsable, previa realización de una evaluación de impacto o EIPD, deberá tener en cuenta una serie de consideraciones para minimizar los riesgos que el tratamiento puede suponer para los derechos y libertades de las personas, adoptando una serie de cautelas y garantías en el diseño de las diferentes operaciones que forman parte del tratamiento:

- **Fase de adquisición de datos:** deberán minimizarse los datos tratados mediante una selección previa de los datos que se requiere recoger y minimizar el grado de detalle con que se tratan recurriendo a la anonimización o seudonimización de las fuentes de origen, el enmascaramiento de los datos o el cifrado de la información.
- **Fase de análisis y validación:** como en la operación anterior, debe minimizarse, en la medida de lo posible, el detalle de los datos mediante técnicas de anonimización y cifrado.
- **Fase de disociación, anonimización o seudonimización de la información**: preferiblemente las personas que lleven a cabo esta actividad no deberán ser las mismas que participen en la fase de explotación de la información, recomendación que se convierte en obligación del responsable cuando se trate de datos de salud como se señala en la disposición adicional decimoséptima de la LOPDGDD, sin perjuicio del resto de obligaciones que se indican en dicha disposición adicional y en particular a la garantía de la trazabilidad de la información en el marco de las garantías prevista en el RGPD. Es preciso señalar que el propio proceso de disociación, anonimización o seudonimización es en sí mismo un tratamiento de datos personales y, por tanto, le es de aplicación las garantías previstas en la normativa de aplicación de datos personales[112].
- **Fase de almacenamiento:** debe garantizarse la confidencialidad de los datos y que estos no son accedidos por terceros no autorizados, recurriendo para ello a técnicas de cifrado y mecanismos autenticación y de control de acceso. También es importante, a fin de evitar posibles inferencias derivadas de un cruce no autorizado de distintas fuentes de información, recurrir a estrategias de distribución de datos que dificulten realizar vinculaciones entre los datos.
- **Fase de explotación:** cuando se vaya a hacer uso de los datos para extraer valor y presentar la información que de ellos deriva, debe garantizarse su anonimización, recurriendo a las diferentes técnicas y, en su caso, a garantías jurídicas dirigidas a

[112] Dictamen 05/2014 sobre técnicas de anonimización

evitar la reidentificación[113], si es que no se ha hecho un uso previo de estas y los datos en esta fase aún siguen permitiendo la identificación de los interesados.

El proceso de agregación para obtener conocimiento implica combinar datos, muchas veces de diferentes fuentes de información, con los riesgos para la privacidad de los interesados que ello representa:

1. **Re-identificación de los individuos o singularización**, aumentando la probabilidad de que esta se produzca cuanto mayor sea el volumen de datos procesados, incluso en aquellos conjuntos de datos que aparentemente pueden no contener identificadores primarios o explícitos[114].
2. **Vinculabilidad** de diferentes registros de un mismo interesado o grupo de interesados, ya sea en el mismo conjunto de datos o a través de la conexión de fuentes de datos heterogéneas e independientes, mediante análisis de correlación.
3. **Inferencia**, a partir de datos personales calificados como cuasi-identificadores[115], de información personal mucho más crítica y que no estaba previsto ser procesada.

Estos riesgos para la privacidad deben de ser evaluados desde la misma concepción del tratamiento que haga uso de técnicas *Big Data* y de sus herramientas analíticas de explotación de información, incorporando, desde el diseño, las estrategias necesarias para mitigarlos y que habrán sido identificadas como resultado de la evaluación de impacto para la protección de datos llevada a cabo.

Cuando se enriquece la información de una misma persona con datos procedentes de distintas fuentes de información probablemente descubramos nuevas conexiones o matices de su personalidad que por separado no se habrían manifestado. Esto es, deducimos y derivamos nueva información sobre el individuo, por lo que, independientemente del propósito concreto del tratamiento, es necesario analizar el riesgo de que puedan producirse inferencias indeseadas, especialmente sobre categorías especiales de datos.

Además, es posible incluso que, al cruzar varias fuentes de datos que supuestamente eran anónimas, por agregación de datos, se revele la identidad de personas concretas: a partir de rasgos generales, el número de individuos en la intersección de todos ellos va disminuyendo, hasta que se identifican personas concretas[116]. Los riesgos de reidentificación se han de medir, evaluar y gestionar tomando las medidas necesarias para reducir la probabilidad de que se materialice dicha reidentificación, previendo incluso posibles medidas reactivas para mitigar el posible daño que pudiera derivarse a una persona física en aquellos casos en los que la reidentificación llegara a producirse. Si se trata de datos de categorías especiales, como los datos médicos, nos encontramos ante una situación de mayor riesgo por el mayor impacto que representa sobre los derechos y libertades de las personas, por lo que las garantías a adoptar han de ser superiores, cuestión que también deberá ser considerada cuando se traten datos de menores o personas en condiciones de especial vulnerabilidad.

---

[113] Se recomienda consultar las publicaciones de la AEPD como: Orientaciones y garantías en los procedimientos de Anonimización de datos personales, la Introducción al hash como técnica de seudonimización de datos personales o La K-anonimidad como medida de privacidad.

[114] Los identificadores primarios o explícitos son aquellos que identifican unívocamente a un individuo, como su número de identificación fiscal, su número de la seguridad social o su número de teléfono móvil.

[115] Los cuasi-identificadores son atributos que no identifican directamente a una persona (fecha de nacimiento, código postal, género, profesión, …) pero que pueden permitir su reidentificación se si combinan o cruzan con otros conjuntos de datos que compartan esos mismos cuasi-identificadores.

[116] El símil más cercano lo tenemos en el juego infantil de '¿quién es quién?' (Guess Who?) en la Wikipedia. https://en.wikipedia.org/wiki/Guess_Who%3F

Si este análisis es importante en el uso interno de los datos por parte de las propias AA.PP., más importante es aún e igualmente se ha de realizar antes de la cesión de datos anonimizados por parte de las AA.PP. a terceros. En caso del que el riesgo de reidentificación sea elevado, dicho tratamiento quedaría sujeto a la normativa de protección de datos y tendría que estar legitimado.

Para el caso de los riesgos relacionados con la reidentificación de los interesados y la inferencia de información resultan útiles las siguientes aproximaciones:

- **Minimización de datos:** el procesamiento de los datos se debe limitar al máximo posible y a lo necesario para alcanzar la finalidad del tratamiento, tanto desde el punto de vista del volumen de población (número de registros) como de datos analizados (atributos procesados).
- **Maximización del nivel de agregación:** se debe evitar en la medida de lo posible reidentificar a los individuos o inferir información sobre ellos dentro del *dataset* o conjunto de datos, para lo cual se precisa minimizar el detalle de la información tratada.
- **Abstracción de la información:** se deben proteger los datos personales y ocultar sus relaciones.
- **Distribución de los datos:** en la medida de lo posible deben distribuirse los datos y procesarse en entornos, si no físicamente, al menos lógicamente separados, con el objetivo de dificultar la inferencia de información por el cruce de datos. Otra aproximación, similar a las técnicas utilizadas en IA, es la utilización de modelos de explotación federados[117].

Para poner en marcha estas estrategias puede recurrirse a diferentes técnicas entre las que destacan las técnicas de anonimización[118] (supresión[119], generalización[120], perturbación[121] y permutación[122] de datos) en el caso de las estrategias de minimización y agregación, y el cifrado de la información para las estrategias de abstracción y distribución de datos[123]. También resultan útiles las técnicas de enmascaramiento[124].

Estas estrategias encaminadas a velar por la anonimización y la disociación de los datos deben complementarse con otras medidas dirigidas a garantizar la transparencia, el control de los usuarios sobre sus datos a través de los mecanismos adecuados para ejercer sus derechos y la aplicación del principio de responsabilidad proactiva por parte del responsable mediante la monitorización, la auditoría y la trazabilidad de las decisiones tomadas y las acciones realizadas.

---

[117] Estos modelos siguen una aproximación "llevar el tratamiento a los datos en vez de los datos al tratamiento" lo que permite gestionar problemas de privacidad, propiedad y localización de los datos.

[118] La AEPD publicó en 2016 las Orientaciones y garantías en los procedimientos de anonimización de datos personales. https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf. También está el Dictamen 05/2014 sobre técnicas de anonimización del Grupo de Trabajo del Artículo 29, detalla estas y otras técnicas de anonimización, su solidez y garantías así como los errores típicos de su aplicación https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf

[119] Mediante la supresión se elimina por completo el valor de un atributo (normalmente identificadores explícitos) o se sustituye por un patrón (por ejemplo "*")

[120] La generalización es una técnica que suele realizarse sobre cuasi-identificadores y que consiste en reemplazar los valores de un atributo por otro valor más abstracto y general dentro de la taxonomía del atributo (por ejemplo, sustituir la edad exacta por un rango de edad o sustituir el código postal completo que identifica el municipio por los dos primeros dígitos que sólo identifican a la provincia)

[121] La perturbación consiste en sustituir los valores originales de los datos (por ejemplo, mediante adición de ruido) de modo que se elimine la vinculación que pueda existir entre los registros originales, pero conservando las propiedades estadísticas de los datos originales.

[122] La permutación consiste en dividir los datos en grupos e intercambiar los valores de los atributos sensibles dentro de cada grupo, de modo que se elimina la relación entre cuasi-identificadores y datos sensibles.

[123] En la guía de Privacidad desde el Diseño, publicada por la AEPD, se describen diferentes estrategias de privacidad orientadas al tratamiento de datos.

[124] Enmascaramiento de datos es el proceso mediante el cual se cambian ciertos elementos de los datos de un almacén de datos, cambiando su información, pero consiguiendo que la estructura permanezca similar, de forma que la información sensible quede protegida. https://www.powerdata.es/enmascaramientode-datos

Tampoco pueden perderse de vista los riesgos que incorporan aquellas soluciones para las que el tratamiento de los datos derive en una toma de decisiones[125]. En ese caso, hay que seguir las mismas recomendaciones que las establecidas en el capítulo sobre IA de este documento.

Por último, y aunque es un 'clásico' de los riesgos en el uso de tecnologías, el sistema debe ser seguro[126] y estar diseñado considerando la protección de datos como un requisito desde el diseño y por defecto[127]. Ni la facilidad para contratar servicios en la nube, ni la variedad y a veces gratuidad de las herramientas para hacer computación masiva, ni el acceso a datos abiertos deben servir de excusa para plantear proyectos donde no se cuida la seguridad y la protección de la información de extremo a extremo y a lo largo de todo el ciclo de vida del tratamiento en operaciones en las que se ven involucrados clientes, proveedores, empleados y los propios usuarios.

[125] El artículo 22 del RGPD establece una prohibición general de adoptar decisiones individualizadas automatizadas basadas en datos personales sensibles (origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos o datos relativos a la salud, vida y orientación sexuales) salvo consentimiento explícito del interesado o por motivos de interés público, siempre que se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades, y los intereses legítimos del interesado.

[126] Artículo 32 del RGPD – Seguridad del tratamiento

[127] Artículo 25 del RGPD – Protección de datos desde el diseño y por defecto

VI. INTELIGENCIA ARTIFICIAL

A. QUÉ ES LA INTELIGENCIA ARTIFICIAL

El término inteligencia artificial o IA se asocia a máquinas o sistemas de información que, en el desarrollo de sus funciones, son capaces de aprender de sus propias experiencias y resolver problemas, más o menos complejos, en diferentes situaciones, de modo que dan la impresión de que 'piensan' o muestran cierta inteligencia[128].

Esta inteligencia, en un proceso como ajustar el enfoque de una cámara[129], puede ser de aparentemente poca importancia, pero también puede ser muy sofisticado como en el caso de un sistema experto de diagnóstico médico. En los últimos años la inteligencia artificial ha salido de los laboratorios y se ha incorporado a múltiples sistemas cotidianos: los buscadores de Internet, la traducción automática, relojes inteligentes, neveras inteligentes, apps de móvil inteligentes, y por supuesto, sistemas inteligentes en las AA.PP..

Bajo el epígrafe de la inteligencia artificial se albergan técnicas muy diversas[130]. Podríamos hablar de reconocimiento del lenguaje natural, de aprendizaje automático, de reconocimiento de patrones, etc. Muchas veces el sistema inteligente es capaz de hacer tareas muy complejas, como jugar al ajedrez o planificar rutas logísticas, pero otras veces se usa en el contexto de pequeñas decisiones que para un humano serían fáciles y repetitivas, permitiendo así reemplazar personas por máquinas. Es el caso de los *chatbots*[131] de texto o telefónicos, para concertar citas o mantener un diálogo cerrado con un usuario, o también los filtros de spam o el reconocimiento de personas en fotografías, o incluso el reconocimiento de expresiones o estados de ánimo.

Otro elemento que ha favorecido la introducción de la inteligencia artificial en muchos procesos es la forma de desarrollar las aplicaciones. Si el desarrollo de programas tradicional se basa en definir un proceso de forma precisa mediante la especificación de una serie de instrucciones elementales, los sistemas basados en aprendizaje automático[132] emplean una técnica distinta. Este desarrollo parte de unas instrucciones más imprecisas de cómo hacer el trabajo[133], pero suficientes como para empezar a operar, y el sistema se 'entrena' con datos de prueba, aprende las relaciones entre las entradas y las salidas, y corrige sus resultados cuando falla, obteniendo al final un sistema que sabe trabajar gracias a su 'experiencia previa'. Esta forma de desarrollar sistemas, que se parece mucho a cómo aprendemos ciertas habilidades los humanos, se lleva bien con algunas tareas difíciles de definir y detallar.

---

[128] El Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial (AI – HLEG) creado la Comisión Europea para desarrollar la Estrategia Europea en Inteligencia Artificial, en su documento "A DEFINITION OF AI: MAIN CAPABILITIES AND DISCIPLINES" propone la aplicación del término de Inteligencia Artificial a "aquellos sistemas que manifiestan un comportamiento inteligente, al ser capaces de analizar el entorno y realizar acciones, con cierto grado de autonomía, con el fin de alcanzar objetivos específicos)

[129] Canon. What is AI-focus https://www.canon.com.au/explore/glossary/ai-focus

[130] La guía "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción", en su apartado "Introducción al marco IA y protección de datos", desarrolla, entre otros, una breve descripción de las técnicas de IA, el ciclo de vida de una solución de IA y de los posibles tratamientos en cada una de estas etapas. https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

[131] Chatbots o bots conversacionales. https://es.wikipedia.org/wiki/Bot_conversacional

[132] Machine Learning: es la capacidad de un sistema inteligente para adaptar y generar nuevas reglas de decisión, a partir de una serie de reglas predefinidas, con el objetivo de mejorar su tasa de acierto.
Deep Learning: sistema de aprendizaje más detallado que Machine Learning que cuenta con varias capas entre la entrada y la salida que le permiten aprender la relación general entre ellas en pasos sucesivos. De esta forma se reduce el margen de error y se aumenta la precisión de las conclusiones, requiriendo un menor grado de orientación humana.

[133] En los ámbitos de la Inteligencia Artificial y aspectos relacionados con la misma como el Machine Learning, el procesamiento de lenguaje natural o la construcción de sistemas expertos se utilizan lenguajes de programación lógica (o declarativa), que describen, a través de algoritmos, la lógica de computación necesaria para resolver un problema sin describir un flujo de control de ningún tipo. Este paradigma se basa en la fórmula "algoritmos = lógica + control" (la llamada Ecuación Informal de Kowalski), lo que significa que un algoritmo se crea especificando conocimiento mediante axiomas (lógica) y el problema se resuelve mediante un mecanismo de inferencia que actúa sobre el mismo (control). https://www.genbeta.com/desarrollo/lenguaje-prolog-ejemplo-paradigma-programacion-logica

Los algoritmos de la IA están pensados para reconocer patrones y así aprender a tomar decisiones de forma autónoma. El uso de estos algoritmos para la toma de decisiones no siempre permite encontrar la traza o explicación a las decisiones tomadas. Este tipo de escenarios se denominan de 'caja negra'[134]. Esta falta de transparencia afecta a distintos aspectos, como es el modo en que toman las decisiones el algoritmo, la influencia de cada elemento de información, la coherencia entre distintas inferencias, la precisión o exactitud de las inferencias o los sesgos introducidos, entre otros. Por ello existe un gran interés en desarrollar metodologías que permitan auditar los algoritmos que infieren nueva información y toman decisiones de forma directa o indirecta, sobre las personas[135].

La inteligencia artificial también despierta dudas entre usuarios, investigadores, especialistas, autoridades y la industria con relación al cumplimiento normativo, la garantía de los derechos de los interesados y la seguridad jurídica de todos los intervinientes. La garantía de los derechos y libertades de los sujetos cuyos datos son tratados por este tipo de soluciones requiere un gobierno de datos adecuado que cubra la calidad e integridad de los datos utilizados, su relevancia a la luz del dominio en el que se desplegarán los sistemas de IA, sus protocolos de acceso, la calidad de los algoritmos utilizados y la capacidad de procesar datos de una manera que se proteja la privacidad.

Además, dado que los modelos de los sistemas de IA se pueden apoyar en enormes cantidades de datos para aprender y realizar la toma de decisiones, cuando se está tratando datos de carácter personal es importante comprender cómo influyen estos datos en el comportamiento de los sistemas y garantizar su calidad e integridad, además de ser necesario evitar que contengan sesgos, inexactitudes, errores y equivocaciones, socialmente construidas, que conduzcan al sistema a extraer generalizaciones incorrectas y a la posibilidad de que tome decisiones injustas que favorezcan a unos grupos sobre otros. Pero, sobre todo, es imprescindible que exista una legitimidad para su tratamiento. Esta necesidad de datos reales puede llevar a un responsable a usar datos recogidos con un propósito distinto e incompatible para entrenar sus sistemas, entrando en conflicto con la licitud[136] y los principios de tratamiento[137].

Muchas veces los sistemas de inteligencia artificial están tratando datos personales e incluso datos especialmente protegidos como los de salud, sexo, raza, creencias u opiniones políticas. Dicho tratamiento puede ir más allá de los datos de entrada, incluyendo datos inferidos que se son obtenidos de dicha información. Para ello, hay que tener muy presentes las restricciones que establece el artículo 9 del RGPD[138] y de la LOPDGDD[139] y las condiciones para levantar dicha limitación.

En cuanto una IA tiene autonomía en la toma de decisiones, hay que tener en cuenta que el RGPD, en sus considerando 71, así como en su artículo 22[140], limita y establece derechos con relación a que los sujetos de los datos no sean sometidos a decisiones exclusivamente

[134] Incapacidad para entender y/o reproducir la decisión tomada por la IA.
[135] La Comisión Europea ha editado en febrero de 2020 un documento llamado On Artificial Intelligence - A European approach to excellence and trust, (https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en). Por su parte el Consejo de Europa ha expresado su preocupación en el documento Artificial Intelligence and Data Protection: Challenges and Possible Remedies (https://rm.coe.int/report-on-artificial-intelligence-artificial-intelligence-and-data-pro/16808e6012). el Ministerio de Ciencia e Innovación, trabaja de forma activa en la elaboración de la Estrategia Nacional de Inteligencia Artificial. http://www.ciencia.gob.es/stfls/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_IDI.pdf
[136] Artículo 6 del RGPD – Licitud del tratamiento
[137] Artículo 5.1.b) del RGPD – Principios relativos al tratamiento. Limitación de la finalidad
[138] Artículo 9 del RGPD - Tratamiento de categorías especiales de datos personales
[139] Artículo 9 de la LOPDGDD – Categorías especiales de datos
[140] Artículo 22 del RGPD - Decisiones individuales automatizadas, incluida la elaboración de perfiles

automatizadas[141] que tengan efectos jurídicos o que afecten significativamente al interesado, incluida la elaboración de perfiles de forma automática[142,143].

Otra de las obligaciones clave que ha de ser tenida en cuenta es la de informar a los interesados y que deberá adaptarse a cada etapa del ciclo de vida de la solución de IA en la que se esté realizando el tratamiento. A este respecto, además de la información que la normativa establece que debe ser proporcionada, resulta de especial interés aquellos casos en los que el interesado esté sometido a decisiones automatizadas o en los supuestos de elaboración de perfiles a los que hace referencia el artículo 22 del RGPD, pues en esos casos el interesado debe disponer de '*información significativa sobre la lógica aplicada'* y '*la importancia y las consecuencias previstas'*.

Como buena práctica, y más allá de exigencias derivadas de la protección de datos, se recomienda la supervisión humana cualificada en cualquier tratamiento basado en IA, y en general, de aquellos que tomen decisiones automatizadas. A la hora de diseñar los sistemas, la supervisión humana es una opción que debe ser tenida en consideración para que forme parte de los procedimientos y mecanismos asociados al tratamiento, de modo que se permita la posibilidad de que un operador humano pueda ignorar el algoritmo en un momento dado. De esta forma, se estaría introduciendo un elemento de control enfocado a dar respuesta al posible riesgo de que la decisión tomada por el sistema no fuera la correcta y estuviera limitando derechos y libertades de los interesados.

Además, es necesario establecer el procedimiento a seguir en aquellas situaciones en las que debe optarse por este modo de actuar, para lo cual es recomendable documentar cualquier petición de intervención humana o de cuestionamiento de la decisión automática recibida de los interesados, de modo que, de su análisis, sea posible detectar situaciones en las que se precisa de esta intervención porque el modelo puede no estar funcionando de la manera esperada.

También podemos encontrar sistemas que están enviando datos personales, sin aplicar ninguna garantía sobre ellos[144], a terceros países que no cuentan con las garantías adecuadas, con el fin de ejecutar parte de las funcionalidades del sistema inteligente en sus servidores.

Para ayudar al cumplimiento del RGPD a aquellas organizaciones que incluyan en sus tratamientos componentes de IA, la AEPD ha publicado el documento Adecuación al RGPD de los tratamientos que incorporan Inteligencia Artificial. Una introducción. en el que se detallan los aspectos de responsabilidad, legitimación, ejercicios de derecho, aplicación de la responsabilidad proactiva, etc.

B. LA IA EN LAS AA.PP.

Es innegable que la inteligencia artificial es una realidad que ha venido para quedarse y que, cada vez más, estará presente en nuestro futuro. El volumen y variedad de datos disponibles y el aumento de la capacidad de proceso son el caldo de cultivo para que se desarrollen soluciones en diferentes áreas o sectores de actividad, entre ellos, el sector

[141] Para ser pueda considerarse que existe participación humana, la supervisión de la decisión ha de ser realizada persona autorizada y competente para modificar la decisión, y ha de realizar una acción significativa y no simbólica.
[142] El Grupo del Artículo 29 ha analizado las implicaciones de este derecho en las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf
[143] Artículo 22 Decisiones individuales automatizadas, incluida la elaboración de perfiles (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e2856-1-1). El GT29 publicó un documento aclaratorio en octubre de 2017 con el título Directrices sobre decisiones individuales automatizadas y elaboración de perfiles
a los efectos del Reglamento 2016/679 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053)
[144] Artículo 46 del RGPD - Transferencias mediante garantías adecuadas

público[145], con el objetivo de automatizar procesos y ofrecer servicios más eficientes y mejorados.

La Comisión Europea, en cumplimiento de su estrategia de IA, ha desarrollado un plan coordinado con los Estados miembros para fomentar el desarrollo y la utilización de la IA en Europa. Este plan incluye la creación de un grupo de expertos sobre inteligencia artificial (AI HLEG, de sus siglas en inglés, *Artificial Intelligence High-Level Expert Group*), compuesto por representantes del mundo académico, la sociedad civil y la industria. Su objetivo es apoyar la implementación de la Estrategia Europea sobre Inteligencia Artificial, teniendo en cuenta diferentes ámbitos que incluyen la protección de datos, y trabajar en la definición de una inteligencia artificial confiable. Para alcanzar esta confiabilidad, la Comisión considera que la IA ha de cumplir con siete requisitos clave: acción y supervisión humanas, solidez técnica y seguridad, gestión de la privacidad y los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y ambiental y rendición de cuentas.

A nivel nacional, el Gobierno de España, trabaja de forma activa en la elaboración de la Estrategia Nacional de Inteligencia Artificial cuyo objetivo es alinear las políticas nacionales destinadas a fomentar el desarrollo y el uso de la IA en España. Sus herramientas son el aumento de la inversión, el refuerzo de la excelencia en tecnologías y aplicaciones de IA, y el fortalecimiento de la colaboración entre el sector público y privado. Su meta es que se produzca un impacto significativo en la sociedad y la economía española.

La Estrategia española de I+D+I en Inteligencia Artificial [146], identifica numerosos campos para el desarrollo de la IA en el sector público, pudiendo citar como alguno de los casos de uso identificados:

- Interacción con el ciudadano, por ejemplo, con el uso de *chatbots*[147,148] basados en el procesamiento del lenguaje natural como primera interfaz entre los ciudadanos y la Administración Pública.
- Salud, tanto para el tratamiento como para gestión.
- Seguridad en temas de vigilancia, movilidad y tráfico o, por ejemplo, a temas concretos como inspecciones de urbanismo.
- Prevención contra la corrupción.

Si bien, con relativa frecuencia, el uso del adjetivo 'inteligente' se asociada a un sistema como sinónimo de avanzado, cuidadoso o personalizado, dando lugar a una etiqueta atractiva para un determinado sistema; paralelamente existen casos del uso fallido de la IA cuando su aplicación se ha basado en expectativas comercialmente atractivas que han supuesto desarrollos y despliegues carentes de un propósito bien definido o adquiridos sin los adecuados análisis de proporcionalidad y necesidad[149].

Cualquier componente IA que se desarrolle no estará aislado y se integrará en un tratamiento específico junto a otros componentes, pudiendo encontrar datos personales en

---

145 https://analiticapublica.es/ia-y-administraciones-publicas?utm_source=inapsocial&utm_medium=pagado&utm_term=nuevo&utm_content=ia&utm_campaign=transformaciondigital

146 Ministerio de Ciencia, Innovación y Universidades – Estrategia Española de I+D+I en Inteligencia Artificial (2019) - http://www.ciencia.gob.es/stfls/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_IDI.pdf

147 Dentro de estos tipos de software o programas informáticos de inteligencia artificial se encuentran los chatbots, que son bots (BOT: programa informático preparado para realizar tareas repetitivas haciendo uso de inteligencia artificial) especializados y creados para mantener conversaciones y ofrecer respuestas preconcebidas.

148 Victoria la Malagueña es un chatbot que ayuda a malagueños y a turistas a conocer la ciudad de Málaga, proporcionando, entre otra, información sobre la ocupación de aparcamientos, información de transporte, información de playas, tiempo, noticias, información de rutas, reseñas de calles, agenda de eventos de la ciudad, y un largo etcétera. https://googlechatbots.es/victoria/

149 También hay decepciones asociadas al 'AI solutionism' (https://towardsdatascience.com/risks-of-ai-solutionism-dangers-of-machine-learning-and-artificial-intelligence-in-politics-and-government-728b7577a243)

las diferentes etapas del ciclo de vida de la solución: entrenamiento, validación, despliegue, explotación y retirada. Es por ello por lo que las AA.PP. que recurran a este tipo de soluciones deben verificar que cumplen un conjunto mínimo de condiciones para garantizar la conformidad del tratamiento realizado, siendo la primera de ellas la existencia de una base jurídica, que puede ser diferente para cada una de las etapas del ciclo de vida de la solución en la que se produzca el tratamiento de datos personales y que pueden ser diferentes.

Hay que tener en cuenta que algunas bases jurídicas, como el interés legítimo, están vedadas para las AA.PP. Esto no implica que si un tercero ha desarrollado un sistema de IA utilizando dicha base jurídica el tratamiento construido sobre la IA no pueda ser empleado por las AA.PP. Lo que sí ocurrirá es que no se podrá utilizar dicha base jurídica por parte de las AA.PP. para justificar tratamientos ulteriores. La selección de las bases jurídicas está estrechamente relacionada con la finalidad del tratamiento y la finalidad perseguida en cada una de las fases del ciclo de vida del sistema y, en el caso de las AA.PP., con sus competencias atribuidas.

C. RIESGOS PARA LOS DERECHOS Y LIBERTADES ASOCIADOS AL USO DE INTELIGENCIA ARTIFICIAL EN LAS AA.PP.

Algunos de los riesgos específicos de la IA están relacionados con el tipo de desarrollo que se utilice. Por ejemplo, si se hace una utilización masiva de datos para entrenar el sistema, como en *Machine Learning*, es conveniente tener en cuenta los mismos riesgos que se han descrito en el caso de los tratamientos basados en *Big Data*.

Los sistemas integran la inteligencia artificial muchas veces en forma de motores y componentes de terceros[150] que se embeben en los tratamientos del responsable interactuando con ellos. Estos componentes embebidos pueden ser simplemente librerías o códigos fuente, pero también puede haber sistemas completos procesando los datos en las máquinas de sus proveedores. Es decir, puedo tener un sistema de información en una AA.PP. pero que integra un motor de inteligencia artificial que se está ejecutando, en tiempo real, en un servidor en Asia, recibiendo los datos y devolviendo los resultados. Esta forma de trabajar 'en la nube' o simplemente con piezas de otros y con varios encargados en cadena, es una fuente de riesgos que deben gestionarse.

Como un tratamiento puede tener una IA en continua evolución y los datos varían con el tiempo, existe el riesgo de que su alcance tenga derivas en la exactitud de la inferencia realizada o que introduzcan sesgos en los resultados.

Además, cuando los modelos de IA contienen en sí mismos datos de carácter personal, existe el riesgo de que algún tipo de ataque pueda desvelar dichos datos personales a terceros. Para ello se pueden utilizar distintas técnicas, similares a las utilizadas para *Big Data*, tanto de privacidad como de seguridad desde el diseño para garantizar la protección de datos personales.

Si el tratamiento basado en IA toma decisiones basadas únicamente en el tratamiento automatizado de los datos explotados, es recomendable que los organismos públicos analicen el riesgo que se deriva de este método de toma de decisiones y adopten mecanismos para su análisis y gestión como:

[150] Como ejemplos más populares de estos motores o *AI engines* podemos citar IBM Watson, Tensor Flow de Google, Amazon Lex o Microsoft Azure Machine Learning. Una buena comparativa de motores puede encontrarse aquí: https://www.agicent.com/blog/best-ai-engines/

- La constitución de comités de ética y protección de datos[151] encargados de evaluar los daños y beneficios potenciales que, para los interesados en particular y para la sociedad en general, pueda suponer un determinado tratamiento.
- Establecer controles periódicos de aseguramiento de la calidad de sus sistemas para garantizar que las personas reciben un trato justo y no discriminatorio.
- Realizar auditorías para comprobar que los componentes utilizados en los sistemas de toma automática de decisiones funcionan según lo previsto[152].
- Para evitar delegar totalmente en la autonomía del sistema y caer en conclusiones que nadie revisa y que pueden tener un gran impacto sobre los derechos y libertades de las personas, es recomendable introducir las garantías de un enfoque subjetivo que explique una verdadera conexión entre los datos y los resultados.
- Implementar mecanismos que permitan al interesado expresar su punto de vista e impugnar la decisión, llegado el caso, con información sobre los plazos acordados para la revisión y un punto de contacto designado para la consulta.
- Incluso cuando se estime que existe una obligación de supervisión humana[153], en los procesos que implican tomas de decisiones automatizadas, hay que evaluar el riesgo de que no exista operador humano cualificado que pueda ignorar el resultado de la decisión tomada en un momento dado. Para ello es clave elaborar procedimientos para aquellas situaciones identificadas como problemáticas en base al análisis de los casos o incidencias en las que el tratamiento no se ha comportado de la manera esperada y en las que debe optarse por la incorporación "de facto" de un supervisor humano que verifique la calidad de la decisión tomada.

Otro riesgo a considerar es que los sistemas de IA pueden ser manipulados para generar inferencias erróneas sobre individuos o grupos de individuos. Estas manipulaciones pueden originarse de fábrica e incluirse como puertas traseras que permitan una manipulación posterior o simplemente ser atacadas explotando posibles vulnerabilidades del sistema. Por lo tanto, hay que evaluar la necesidad de realizar auditorías para detectar estas vulnerabilidades, y en su caso, planificarlas definiendo su periodicidad y alcance.

Tampoco debe perderse de vista que durante la operación del sistema se puede crear un efecto "criterio de autoridad" en el que los operadores encargados de interactuar con la solución no revisen críticamente las decisiones o inferencias generadas por la IA y que se pierda la característica de una supervisión humana realmente cualificada, o que incluso,

---

[151] En la estrategia de I+D+i en IA del Gobierno de España se plantea, en el desarrollo de la prioridad 1 la involucración del Comité Español de Ética en la Investigación en el uso e implementación de la IA desarrollándolo en la prioridad 6 en la que destaca que el mismo debe liderar las actividades de análisis y valoración de los aspectos éticos del uso e implantación de la IA en las actividades desarrolladas en los Planes Estatales de I+D+I.
(https://www.ciencia.gob.es/stfls/MICINN/Ciencia/Ficheros/Estrategia_Inteligencia_Artificial_IDI.pdf)
Ya existen iniciativas en este sentido, como el Comité de Ética de la Inteligencia Artificial creado por la Mutualidad de la Abogacía para los sectores financieros y aseguradores (https://www.mutualidadabogacia.com/sala_de_prensa/cronica-comite-etica-presentacion/)

[152] La pandemia de COVID-19 y la ausencia de exámenes presenciales ha obligado a las autoridades académicas del Reino Unido a utilizar un algoritmo para calificar a los alumnos en los exámenes GCE de acceso a los estudios universitarios. El algoritmo, además de tener en cuenta factores coherentes, como el historial del estudiante, ha incluido otros más polémicos cómo el propio historial de sus compañeros y del centro al que pertenece el estudiante, dando lugar a multitud de críticas al demostrarse que el algoritmo ha sido particularmente injusto con las minorías étnicas de entornos más pobres y desfavorecidos que han visto sus notas rebajadas en comparación con los estudiantes de zonas más ricas. https://www.xataka.com/robotica-e-ia/cuando-nota-no-te-pone-profesor-sino-algoritmo-caos-estudiantes-reino-unido

[153] De acuerdo con el artículo 22.3 del RGPD, en la celebración o ejecución de contratos entre el interesado y el responsable del tratamiento o si este se basa en el consentimiento explícito del interesado, el responsable debe adoptar las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado y, como mínimo, el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

aunque se revise dicha decisión, esta quede registrada como errónea y cree dudas o sesgos en futuras decisiones humanas. La necesidad de supervisión humana debe de entenderse como una forma de mejora continua de los procesos de IA en la que debe de estar involucrado todo el personal implicado en el marco del tratamiento realizado.

Para los *chatbots* o diálogos inteligentes usados en los canales de comunicación con la Administración se corre el riesgo de que no resulten accesibles para personas con discapacidades. En estos casos, se debe evaluar el riesgo de que no exista una forma racional y natural, a través de interlocutores humanos, de dirigirse a la Administración para estudiar y hacerse cargo de estos casos, evitando así posibles riesgos de discriminación resultantes del uso de la IA.

Además de este, los *chatbots* tienen otros riesgos, como el de recoger y distribuir información de carácter personal a terceros en caso de tener un modelo de aprendizaje continuo sobre la información proporcionada por los usuarios. En el mismo caso, si el algoritmo evoluciona sin supervisión, existe el riesgo de que pueda cambiar su modelo de razonamiento hacia inferencias erróneas. Los *chatbots* pueden tener vulnerabilidades de seguridad y ser utilizados por hackers para acceder a información personal[154], también pueden recoger más información de la necesaria, incluir sesgos que afecten a la calidad de datos o realizar inferencias sobre categorías especiales. Estos riesgos son más acusados cuando dichos *chatbots* son empleados para dar asistencia sobre temas de salud mental o atención a víctimas y menores.

En cuanto a la auditoría anteriormente señalada[155], dada la dificultad para analizar el comportamiento real de estos sistemas, no siempre basta con un análisis de los requisitos o unas pruebas previas a la operación, sino que es preciso auditar de forma continua que los resultados obtenidos son adecuados y evolucionan de acuerdo con los cambios sociales.

[154] Sus vulnerabilidades pueden ser empleadas para implementar ataques de ingeniería social: https://venturebeat.com/2017/05/29/what-happens-when-hackers-attack-chatbots/

[155] La realización de auditorías, como instrumento para verificar el cumplimiento de las obligaciones impuestas por la normativa al responsable del tratamiento, aparece explícitamente recogido en el artículo 28.3.h) del RGPD relativo al encargado del tratamiento y en el artículo 39.1.b) relativo a las funciones del delegado de protección de datos.

VII. BLOCKCHAIN Y TECNOLOGÍAS DE REGISTRO DISTRIBUIDO

A. QUÉ ES EL BLOCKCHAIN

El *blockchain* o cadena de bloques[156], DLT o Bitcoin son términos que han irrumpido con fuerza en los últimos tiempos y que han despertado mucho interés en los últimos años. Los tecnólogos y muchas personas se han visto sorprendidos por la novedad de las monedas virtuales como el Bitcoin[157], y por su aparente transparencia e integridad de la información almacenada.

De una forma simple, podemos definir *blockchain* como una red de participantes (pares, *peers* o nodos) que comparten un registro de forma distribuida en el que se apunta quién posee qué (activos) y quién negocia con quién (transacciones). A diferencia de los tradicionales sistemas centralizados en los que las bases de datos están controladas por una única autoridad central, en *blockchain* todos los nodos mantienen una copia de este registro por lo que resulta extremadamente complicado manipular la información anotada sin que la red, entendida esta como el conjunto de los participantes, sean conscientes del intento de cambio. *Blockchain* toma su nombre por la forma en que se organiza ese registro: un conjunto de bloques en los que se agrupan las transacciones y que están enlazados unos con otros, en orden cronológico, a través de un mecanismo criptográfico llamado hash que garantiza la integridad y la inmutabilidad de la información registrada en la cadena.

Blockchain es un caso particular de un concepto más amplio que son las tecnologías de registro distribuido o DLT por sus siglas en inglés *Distributed Ledger Technology*, que hacen referencia a bases de datos distribuidas y descentralizadas gestionadas por varios participantes, normalmente equivalentes desde el punto de vista de autoridad. Al carecer de una entidad central que ejerza las funciones de verificación y validación de la información se recurre al establecimiento de mecanismos de consenso entre los participantes para decidir cómo se toman las decisiones, se actualizan los datos y se mantiene la información almacenada en un estado consistente.

Los promotores del *blockchain* apuestan por un futuro en que no hacen falta intermediarios o fedatarios que custodien una cuenta, un contrato o un registro. Todas las transacciones se anotarían en cadenas aparentemente inmutables y transparentes que incluso se podrían actualizar de manera automática a través de contratos inteligentes[158] albergados en la propia cadena (los llamados *smart contracts*).

Existen varios tipos de *blockchains,* pero todas ellas comparten, en mayor o menor grado, unas características comunes: transparencia, inmutabilidad, descentralización, integridad y confianza. Estas características hacen posible uno de sus principales atractivos, como es la eliminación de intermediarios en el procesamiento de transacciones entre partes, lo que es también una de sus principales debilidades a la hora de establecer garantías jurídicas a su operación.

Para avanzar hacia este escenario se han promovido varias infraestructuras de cadenas de bloques, que difieren unas de otras en la visibilidad o alcance de sus operaciones (públicas o privadas) y en la forma de gestión del *blockchain* (permisionado o no-permisionado).

[156] La Wikipedia proporciona una buena introducción https://es.wikipedia.org/wiki/Cadena_de_bloques
[157] Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto https://bitcoin.org/bitcoin.pdf
[158] https://es.wikipedia.org/wiki/Contrato_inteligente

Como con cualquier otra tecnología, una implementación de *blockchain* puede estar tratando en exclusiva información que no tenga datos personales como, por ejemplo, un registro de movimiento de mercancías[159]. Sin embargo, en cuanto una red *blockchain* se emplee para la custodia de datos personales, es evidente que el tratamiento en el que se incluya precisa cumplir con los requisitos establecidos en el RGPD, entre otros, una clara identificación de los responsables (y otros roles), una legitimación para el tratamiento, garantías de confidencialidad y disponibilidad de los datos y la posibilidad de ejercer unos derechos por parte del interesado.

Otra cuestión para considerar en el despliegue de este tipo de redes es cómo se van a ver afectadas por la ubicación de los datos. El RGPD es muy claro respecto a las transferencias de datos entre países con diferente nivel de protección[160], y la idea de una red de almacenamiento deslocalizada no facilita mucho la aplicación de esas garantías. Por otra parte, los algoritmos de cifrado de información son cada día más robustos, pero también cada día descubrimos cómo la presunta robustez de hace unos años ahora se rompe usando equipos cada vez más accesibles.

Antes de poner en marcha un proyecto *blockchain* ha de analizarse la compatibilidad de la solución con las exigencias normativas impuestas por el Reglamento General de Protección de Datos[161]. En concreto, han de analizarse con cuidado los siguientes aspectos:

- **Responsabilidad del tratamiento**[162]. La cadena de bloques, aunque depende del tipo de red *Blockchain* implementada, es, por definición, un sistema descentralizado donde es difícil identificar al responsable (o responsables) del tratamiento.
- **Derecho al olvido**[163] **y rectificación**[164]**.** Uno de los principios en los que se basa *blockchain* es la imposibilidad de alterar el contenido sin producir una inconsistencia, por lo que la existencia de soluciones para la eliminación o modificación de información registrada deben ser cuidadosamente analizadas
- **Conservación limitada de los datos**[165]**.** Uno de los principios de tratamiento de los datos personales es que *"estos solo deben mantenerse de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales"* por lo que es necesario implementar mecanismos alternativos que den solución a la inmutabilidad propia de la red.
- **Seguridad**[166]**.** En algunas implementaciones de *blockchain*, existen dos aspectos de seguridad importantes que pueden estar en riesgo. El primero es la confidencialidad de los datos al exponerse información en la red. El segundo, y menos obvio es el de disponibilidad pues, aunque en principio la información está distribuida en muchos nodos, en general, no existe siempre una garantía de la disponibilidad de dichos nodos (acuerdos de nivel de servicio), ni siquiera de un

[159] Existe y está bastante actualizado un Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea (https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018R1807&from=EN)

[160] El capítulo V del Reglamento General de Protección de Datos se dedica íntegro a las transferencias internacionales de datos.

[161] Blockchain and Data Protection in the European Union, Michèle Finck, Max Planck Institute for Innovation and Competition; Universidad de Oxford, febrero 2018 https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3119584_code1137858.pdf?abstractid=3080322&mirid=1

[162] Artículo 24 del RGPD – Responsabilidad del responsable del tratamiento

[163] Artículo 17 del RGPD – Derecho de supresión

[164] Artículo 16 del RGPD – Derecho de rectificación

[165] Artículo 5.1.e) del RGPD – Principios relativos al tratamiento. Limitación del plazo de conservación

[166] Artículo 32 del RGPD – Seguridad del tratamiento

compromiso de su existencia futura. Esto ocurre especialmente en el caso de implementaciones de redes *blockchain* públicas.

- **Transferencias internacionales de datos**[167]. Debe tenerse presente que el uso de *blockchain* como solución tecnológica en muchos escenarios puede derivar en la existencia de transferencias internacionales de datos por la propia naturaleza de la tecnología y especialmente en el caso de uso de redes *blockchain* públicas. Una buena forma de abordar este riesgo es aplicar los principios de privacidad desde el diseño, elegir cuidadosamente tanto el tipo de red a utilizar (optar por redes *blockchain* híbridas o privadas) así como el modelo de gobernanza de la información (por ejemplo, almacenamiento *off-chain* de los datos).

B. EL BLOCKCHAIN EN LAS AA.PP.

La aplicabilidad práctica del *blockchain*, al margen de las criptomonedas y aquellos entornos en donde se carece de seguridad jurídica, se ha encontrado con problemas para su despegue. Es el caso de las AA.PP. cuando actúan en el marco de sus competencias. Su actuación se caracteriza por la existencia de un marco legal regulador y el reconocimiento de la figura de un tercero de confianza, lo que difiere bastante del enfoque de *blockchain*.

Sin embargo, se han desarrollado un gran número de iniciativas[168] y pruebas de concepto de posibles usos del *blockchain* tanto en las empresas como en las AA.PP. Respecto a estas últimas, en muchos lugares del mundo han aparecido proyectos piloto como, por ejemplo, registros de propiedad, de títulos y de ofertas, trazabilidad de productos alimenticios, o gestión de identidades o voto electrónico.

Al igual que comentábamos con las anteriores tecnologías, si su uso implica publicar contenidos propios de la Administración que pueden contener datos personales tanto de los ciudadanos como de los empleados públicos, se tendrán que cumplir lo establecido en el RGPD.

El 10 de abril de 2018, los Estados miembros de la UE y Noruega firmaron una declaración conjunta para crear la Asociación Europea de Blockchain (por sus siglas en inglés, EBP)[169] y acordaron cooperar en el establecimiento de una Infraestructura Europea de Servicios de Blockchain (por sus siglas en inglés, EBSI) encargada de respaldar la entrega de servicios al público digital transfronterizo, con los más altos estándares de seguridad y privacidad. Algunos gobiernos[170] e instituciones públicas están desarrollando estrategias o proyectos con *blockchain* como:

- **Titulaciones:** Devolver el control a los ciudadanos a la hora de gestionar sus credenciales educativas; reducir significativamente los costes de verificación y mejorar la confianza en la autenticidad, evitando los fraudes en los títulos oficiales, propietarios y certificaciones privadas.
- **Notaría:** Aprovechar el poder de *blockchain* para crear registros compartidos de documentos de auditoría digitales, automatizar las comprobaciones de cumplimiento en procesos sensibles al tiempo y demostrar la integridad de los datos.
- **Identidad Europea Auto soberana**: Permite a los usuarios crear y controlar su propia identidad a través de las fronteras sin depender de las autoridades centralizadas. El objetivo del proyecto es que los ciudadanos puedan gestionar y

[167] Artículo 44 del RGPD – Principio general de las transferencias
[168] EU-Funded Projects in Blockchain Technology https://ec.europa.eu/digital-single-market/en/news/eu-funded-projects-blockchain-technology
[169] European Blockchain Services Infrastructure (EBSI) - https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI
[170] Malta, Alemania, Australia, Reino Unido, Finlandia, Suecia, cuentan con proyectos realizados sobre tecnología blockchain.

ser propietarios de su identidad digital y decidir quién puede tener acceso a sus datos y a cuáles.

- **Intercambio de datos de forma fiable:** Aprovechar la tecnología de *blockchain* para compartir de forma segura los datos entre las autoridades aduaneras y fiscales de la UE.

La Comisión Europea desplegó en 2019 una red piloto para testar todos los casos de uso mediante una historia de usuario titulada 'El viaje de Eva'[171] desarrollada sobre la Infraestructura de Servicios Blockchain Europea (EBSI), y están desarrollando nuevos casos de uso.

A nivel nacional, también se están desarrollando diferentes proyectos piloto y pruebas de concepto para analizar el potencial que la tecnología podría tener en el sector público e identificar aquellos casos concretos en los que su uso podría efectivamente mejorar la prestación de los servicios prestados a la ciudadanía, entre otros:

- **Certificaciones Académicas:** En el contexto del proyecto de Titulaciones desarrollado en la EBSI, la CRUE-TIC, a través de la red BLUE (red Blockchain de Universidades Españolas) está desarrollando una prueba de concepto para registrar las titulaciones académicas, así como las competencias y otras habilidades formativas y que permitirá que los estudiantes puedan gestionar su intercambio con los agentes del sector involucrados.
- **Registro electrónico de apoderamientos:** El Ayuntamiento de Bilbao está en fase de desarrollo de una red *blockchain* y una aplicación informática para gestionar el REA (Registro Electrónico de Apoderamientos) interoperable con el resto de los registros de las AA.PP. con el fin dar cumplimiento a lo previsto en el art. 6 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las AA.PP.. Para ello, se apoya sobre la plataforma existente desplegada por la Sociedad Informática del Gobierno Vasco -EJIE (Eusko Jaurlaritzaren Informatika Elkartea) que adjudicó, a finales de 2017, un contrato cuyo objeto era el desarrollo e implantación de una solución *blockchain* para cubrir escenarios ligados al registro de contratistas del Gobierno Vasco.
- **Registro de licitaciones y evaluación automatizada:** en una línea similar, la Dirección General de Contratación, Patrimonio y Organización del Gobierno de Aragón está desarrollando un servicio de registro distribuido de ofertas y evaluación automatizada de las mismas en procedimientos de contratación pública electrónica que licitó a finales de 2018 con el objetivo de aumentar la transparencia y la seguridad en procedimientos de licitación pública.

El *blockchain* es una pieza más en el conjunto de un tratamiento, pero no reemplaza al resto de los elementos organizativos y técnicos que conforman dicho tratamiento. Como en todo proyecto que implique el desarrollo de un nuevo servicio o una nueva implementación del mismo, ha de estar sometido a un análisis de idoneidad, proporcionalidad y necesidad[172]. Si tras un análisis preliminar sobre la viabilidad y adecuación técnica y normativa el organismo decide optar por el desarrollo de una aplicación o servicio sobre este tipo de tecnología, deberá realizar un análisis cuidadoso del tratamiento que desee llevar a cabo y entender el contexto, alcance e implicaciones de este a fin de identificar y evaluar cualquier posible riesgo para los derechos y libertades de las personas físicas que pueda surgir.

En lo que se refiere al desarrollo de proyectos sobre tecnologías DLT, hay que tener en cuenta el Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de

[171] Hay un video muy ilustrativo en https://www.youtube.com/watch?v=m2uj7fgb2JI

[172] Blockchain Technology Overview. Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone. En la página 42 de este documento hay un interesante flujograma sobre la viabilidad de proyectos con Blockhain. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf#page=53

julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, conocido como Reglamento eIDAS y el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones,

Este último, a fin de garantizar la seguridad pública en relación con el empleo de sistemas de identificación y firma electrónica, establece la obligatoriedad de que, en relación con los sistemas previstos en la letra c) del apartado 2 de los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, es decir, los sistemas de clave concertada y cualquier otro sistema que las Administraciones consideren válido en los términos y condiciones que se establezca para que los interesados puedan identificarse electrónicamente ante las AA.PP., los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en territorio español en caso de que se trate de las categorías especiales de datos a los que se refiere el artículo 9 del RGPD. Estos datos, salvo las excepciones que se introducen en la ley, no podrán ser objeto de transferencia a un tercer país u organización internacional y, en cualquier caso, se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Adicionalmente, el artículo 3 del mencionado Real Decreto-Ley incorpora una disposición adicional sexta a la Ley 39/2015, de 1 de octubre, que prevé que en las relaciones de los interesados con las AA.PP. no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificaciones basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea. Además, la nueva disposición adicional sexta establece que cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal deberá contemplar que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública.

C. RIESGOS PARA LOS DERECHOS Y LIBERTADES ASOCIADOS AL BLOCKCHAIN

Previo a la implementación de una solución basada en *blockchain* que exija el tratamiento de datos personales es necesario valorar, en el marco de una evaluación de impacto para la protección de datos, la necesidad y la proporcionalidad del empleo de esta tecnología frente a otras posibles alternativas y los riesgos adicionales que introduce por su propia definición y diseño.

Otra decisión importante, una vez que se ha optado por *blockchain* como solución tecnológica, tiene que ver con la elección del tipo de red que se va a implementar como soporte al tratamiento. Si ya se dispone de un proyecto de tratamiento que cumple con lo establecido en el RGPD, hay que evaluar el riesgo que supone, en vez de optar por una red *blockchain* privada y gobernada que esté bajo el total control de una AA.PP., elegir otros tipos de *blockchain*.

La implementación de *blockchain* sobre los servicios ofertados exige a las AA.PP. la necesidad de realizar un juicio de proporcionalidad, evaluando los principales beneficios sobre los servicios ofrecidos frente a los principales retos en materia de protección de datos mencionados anteriormente. Es responsabilidad de la Administración Pública evaluar si la solución tecnológica adoptada es la más adecuada o, por el contrario, introduce riesgos que no permitan ser gestionados. En particular, es importante evaluar qué tipo de arquitectura de red *blockchain* se adapta mejor a la solución (públicas, privadas, permisionadas y no permisionadas) ya que no todas ellas representan el mismo nivel de riesgo, además de definir el modelo de gobernanza más adecuado. No debe perderse de vista que la no

posibilidad de cumplir técnicamente con alguna de las obligaciones exigidas por el RGPD al responsable no debe ser considerada un riesgo susceptible de tratar sino un incumplimiento normativo.

En el caso de que la red *blockchain* utilizada se apoye en un mecanismo de gobernanza que no esté bajo el control de la AA.PP., hay que prever que se pueden introducir cambios que pongan en peligro los principios y derechos de protección de datos. A su vez, hay que determinar si existe un riesgo de que los niveles de calidad de servicio, en cuanto a disponibilidad de los nodos o tiempos de respuesta, no se cumplan. En unn caso extremo, podríamos encontrarnos ante una situación en la que los nodos de la red de *blockchain* cesaran en su actividad. Por ello, además de las garantías jurídicas, hay que disponer de planes de contingencia que garanticen la continuidad del tratamiento y que podrían incluir, por ejemplo, opciones de portabilidad para asegurar que al menos los derechos de los administrados se pueden proteger.

La seguridad de *blockchain* se apoya fundamentalmente en la robustez de sus mecanismos criptográficos. Todo sistema criptográfico tiene un tiempo de vida limitado e indeterminado. Por lo tanto, hay que gestionar el tiempo de obsolescencia y la posibilidad de que en un momento dado todo el sistema se pueda ver comprometido.

La naturaleza del sistema distribuido hace más complejo realizar un control del acceso a los datos, así como la llevanza de un registro de accesos. Esta circunstancia se puede agravar cuando el modelo de *blockchain* elegido permita la entrada y salida dinámica de participantes.

En relación con este punto y la configuración dinámica de participantes en *blockchain*, es necesario gestionar el modelo elegido de mecanismo de consenso a la hora de generar la cadena de bloques y evaluar de forma continua el riesgo de manipulación.

En virtud de la protección de datos por diseño[173], una estrategia de seudonimización es limitar la información volcada en a la red *blockchain* a *commitments* o compromisos[174] y si esto no fuera posible, en forma de hashes[175] utilizando una función hash con una clave o, al menos, en forma de cifrado de modo que se garantice la confidencialidad de la información registrada en la cadena. Se ha de evitar la publicación de datos personales en claro en la cadena de bloques, los cuales deberían alojarse *off-chain,* en bases de datos tradicionales u otros sistemas de información del responsable.

No hay que olvidar que *blockchain* es la solución, o una de las soluciones tecnológicas, que dan soporte a un tratamiento de datos, en cuyo marco existirán otras herramientas para el acceso, la gestión e incluso, mecanismos de intermediación para usuarios. Todos estos elementos tienen sus propias vulnerabilidades, en concreto de seguridad, por lo que se han de analizar los riesgos e implementar las medidas necesarias para evitar la suplantación de identidad en la ejecución de las transacciones[176] [177] [178] [179] y garantizar una seguridad integral.

---

[173] Artículo 25 del RGPD – Protección de datos desde el diseño y por defecto

[174] Un esquema de compromiso (o commitment scheme) es un método criptográfico que permite enviar información secreta, que permanece oculta para otros y cuyo resultado se revela en una etapa posterior, de modo que sean vinculantes y no pueda alterarse en una etapa posterior ni por el emisor ni por el receptor. Un ejemplo muy común son las pruebas de conocimiento cero (o ZKP del inglés Zero Knowledge Proof)

[175] En el estudio “Introducción al hash como técnica de seudonimización de datos personales” publicado por la Agencia Española de Protección de Datos, se explica en qué consiste una función hash, su utilidad como técnica de seudonimización así como sus riegos y límites de uso. https://www.aepd.es/sites/default/files/2020-05/estudio-hash-anonimidad.pdf

[176] https://es.cointelegraph.com/news/cisco-and-ukrainian-cyber-police-uncover-50-mln-bitcoin-phishing-scam

[177] https://criptomonedaseico.com/noticias/los-ciberdelincuentes-generan-bitcoin-utilizando-la-estafa-falsa-de-la-pagina-web-de-la-bbc/

[178] https://www.criptonoticias.com/seguridad-bitcoin/detectan-campana-phishing-robar-bitcoins-basada-dominio-blockchain-info/

[179] A. A. Andryukhin, "Phishing Attacks and Preventions in Blockchain Based Projects," 2019 International Conference on Engineering Technologies and Computer Science (EnT), Moscow, Russia, 2019, pp. 15-19, doi: 10.1109/EnT.2019.00008. https://www.researchgate.net/publication/333072391_Phishing_Attacks_and_Preventions_in_Blockchain_Based_Projects

VIII. SMARTCITIES O CIUDADES INTELIGENTES

A. QUÉ SON LAS CIUDADES INTELIGENTES

El concepto de ciudad inteligente o *Smart City*[180] ha sido utilizado por la Comisión Europea para agrupar un conjunto de proyectos tecnológicos muy diversos orientados optimizar la gestión de recursos en las ciudades[181] mediante el uso de la tecnología aplicada a gestionar, de una manera más eficiente, los servicios típicos de una ciudad, como son los transportes, infraestructuras, suministros de luz, agua y gas, gestión de los residuos o ayudas sociales.

Los proyectos más característicos de ciudades inteligentes se basan, en primer lugar, en la recogida de datos de forma automatizada mediante sensores, de diversos tipos, distribuidos en la ciudad: de tráfico, de movimiento de personas, de calidad del aire, de consumos energéticos, etc. A continuación, se procede al análisis automatizado de dichos datos, que puede realizarse de forma integrada e incluso enriqueciendo los datos de otras fuentes. Si estos datos se combinan adecuadamente pueden servir para dimensionar y predecir qué servicios y en qué cantidad hay que ofrecer. Finalmente, se dispone de una fase de elaboración de conclusiones o decisiones que podrían, en algunos casos aplicarse, de forma automatizada mediante activadores, por ejemplo, para regular el tráfico rodado en una gran ciudad, y que pueden implicar otras tecnologías de las revisadas en este documento como la inteligencia artificial.

Es decir, aunque se puede hablar de tecnología *Smart City*, esta se podría considerar como la integración con un propósito de gestión urbana de distintas tecnologías como técnicas de inteligencia artificial y *Big Data*, que también aparecen en este documento, y, en particular, el desarrollo de proyectos de IoT[182] (*Internet of Things* o Internet de las cosas).

B. SMART CITY Y LAS AA.PP.

En el marco de las competencias de las AA.PP. de realizar una prestación de servicios de calidad al ciudadano con la mayor eficacia posible y de forma sostenible, la tecnología *Smart City* ofrece a los responsables de los municipios la capacidad de obtener información, en tiempo real mediante sensores o fuentes de datos de determinados servicios, del comportamiento de las ciudades y de sus habitantes. Algunas fuentes de datos podrían ser contadores inteligentes de transeúntes, uso de datos de telefonía móvil, de los datos de las tarjetas de transporte, entre muchísimos otros.

Recientemente el IESE Business School de Navarra publicó su sexta edición del informe *Cities in Motion Index* (CIMI)[183] correspondiente al año 2019. El estudio evalúa aspectos de 176 de las principales ciudades del mundo[184] con el objetivo de puntuar y comparar, entre otros aspectos, el uso de tecnologías que mejoran la calidad de vida y facilidades para sus ciudadanos. Estas son algunas aplicaciones reales que se encuentran en las mencionadas urbes:

- **Eficiencia energética en instalaciones:** mediante la instalación de cámaras o sensores que detecten la presencia de personas en la instalación y, en

[180] Una vez más los redactores de la Wikipedia han hecho un buen trabajo buscando definiciones y referencias. https://es.wikipedia.org/wiki/Ciudad_inteligente

[181] Web de Smart cities/Smart living de la Comisión Europea. https://ec.europa.eu/digital-single-market/en/smart-cities

[182] Una introducción a la Internet de las Cosas https://es.wikipedia.org/wiki/Internet_de_las_cosas

[183] Se puede consultar el informe del IESE Business School – Cities in Motion en el siguiente enlace: https://media.iese.edu/research/pdfs/ST-0509-E.pdf

[184] Varias ciudades españolas se han visto incluidas en dicho listado, en concreto ocupando los puestos en el ranking mundial: Madrid (24), Barcelona (28), Valencia (61), Sevilla (76), Málaga (80), Palma de Mallorca (88), Zaragoza (101), A Coruña (102), Murcia (105), Bilbao (107).

consecuencia, encender las luces o poner en funcionamiento el sistema de refrigeración.

- **Movilidad y gestión eficiente del tráfico:** instalando cámaras y sensores en puntos estratégicos que permitan contabilizar las personas y vehículos que hay en la zona, dando prioridad a unos u otros en función del volumen y necesidad.

- **Eliminación de residuos a través de sistemas de basura inteligentes:** se usan sensores que detectan los niveles de basura en los contenedores y notifican a los camiones de eliminación de desechos cuando es el momento de recoger, reduciendo así la contaminación acústica de los camiones de basura y reduciendo costes al desarrollar rutas más eficientes adaptadas al nivel real de residuos generados en cada lugar.

En el último ejemplo podemos apreciar que no todos los datos procesado en una ciudad inteligente son personales. Además, el cumplimiento de los objetivos de eficiencia de las *Smart Cities* no justifica una recogida masiva e indiscriminada de datos personales. Atendiendo al principio de minimización[185], los datos recopilados han de ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

La finalidad de la información recogida puede ser la de ejecutar tanto la función pública como la investigación científica o fines estadísticos. En dichos casos, hay que tener en cuenta la compatibilidad de estos últimos tratamientos con los fines anteriores, como se establece en el artículo 5.1.b y en el 89 del RGPD, siempre que estén sujetos a las garantías adecuados. Por ejemplo, a la hora de la recogida automática, en tiempo real, de información con propósito estadístico, entre otras medidas legales, técnicas y organizativas, se ha de analizar el tamaño de la muestra, determinada por el número de sujetos o elementos de una población necesarios para que los datos obtenidos sean representativos y eficaces. La cantidad de datos personales recogidos, entendida tanto como la extensión del número de sujetos como el conjunto de datos recogidos de un mismo sujeto, se han de someter a un análisis de proporcionalidad y necesidad.

En este sentido, para muchos tratamientos vinculados a la *Smart City* no parece necesario identificar unívocamente a los ciudadanos, sino que se podría cumplir con la finalidad empleando datos anónimos y agregados. Para predecir cuándo y dónde se producen los picos de tráfico, dónde es necesario optimizar el suministro energético o dónde hay que mejorar la recogida de residuos no hacen falta tratar los identificadores de las personas que reciben estos servicios.

Las AAPP, atendiendo al principio de minimización y teniendo en cuenta la necesidad y proporcionalidad del tratamiento, deberán analizar si se requiere identificar a los ciudadanos, valorado si es suficiente para los objetivos del tratamiento el uso de datos anónimos y agregados. Para predecir cuándo y dónde se producen los picos de tráfico, dónde es necesario optimizar el suministro energético o dónde hay que mejorar la recogida de residuos hay que evitar el uso de identificadores de las personas que reciben estos servicios.

Otro aspecto a tener en cuenta es que se ha de atender al principio de lealtad[186] del tratamiento, es decir, que los datos recogidos se van a utilizar para la finalidad perseguida y el propósito original. Por ejemplo, cuando un tratamiento tiene como objeto el garantizar que una determinada área de la ciudad tiene restricciones de acceso, hay que diferenciar el propósito de controlar dicho acceso de lo que es la actividad sancionadora de aquellos que no cumplen con dichas restricciones. Por lo tanto, el tratamiento ha de buscar la máxima efectividad en el propósito original siendo proporcional al grado de intrusión en la privacidad

[185] Artículo 5.1.c) del RGPD – Principios relativos al tratamiento. Minimización de datos
[186] Artículo 5.1.a) del RGPD – Principios relativos al tratamiento. Licitud, lealtad y transparencia

de los administrados, no debe centrarse exclusivamente en buscar la máxima eficiencia en uno de sus instrumentos de aplicación.

Para gestionar una colección de proyectos como los asociados a las ciudades inteligentes podría requerir de la colaboración de AA.PP. con empresas privadas y otros colectivos, que intercambien datos entre ellos. Este intercambio requiere de formatos interoperables y datos accesibles.

Otra cuestión que debe resolverse en proyectos como estos, en los que varios intervinientes realizan una parte del tratamiento, es quién toma las decisiones en cada momento actuando como responsable del tratamiento[187]. También es importante clarificar quiénes son los corresponsables[188] y encargados[189] y cómo se formaliza la relación entre ellos. En concreto, es preciso delimitar qué datos emplea cada una de las partes y para qué.

Siempre que se recojan datos de personas y, aunque después se anonimicen, es preciso informarles[190] adecuadamente del marco del servicio en el que se produce esta recogida, de qué datos se recogen y para qué y de cómo pueden ejercer sus derechos sobre los mismos. La página web de la Administración Pública puede ser un buen lugar para publicar y sobre todo para mantener actualizada esta información.

Los ciudadanos son una parte esencial de un proyecto *Smart City*. El proporcionarles la información adecuada respecto a la recogida y uso de los datos, más allá del cumplimiento estricto de los artículos 13 y 14 del RGPD y de la aplicación de los principios de privacidad desde el diseño tal y como recoge el Considerando 39, permite a los ciudadanos tener conocimiento de los riesgos, las normas, las salvaguardas y los derechos relativos al tratamiento de datos personales así como del modo de ejercer sus derechos en relación con el tratamiento, aumentando así su nivel de confianza y compromiso con el proyecto. La página web de la AA.PP. es también un buen lugar para dar a conocer proyectos específicos de compartición de datos con otras entidades públicas o privadas y así aclarar y extender aspectos de la finalidad y dar a conocer el valor añadido que se pretende conseguir con estos proyectos. Las demandas de generación de datos abiertos e intercambio de datos con terceras partes deben de compatibilizarse con los principios de trasparencia que permiten preservar la legitimización del tratamiento.

C. RIESGOS PARA LOS DERECHOS Y LIBERTADES ASOCIADOS A LAS CIUDADES INTELIGENTES

A la hora de redactar los contratos entre responsables, corresponsables y encargados es importante tomar en cuenta que los proyectos de Smart City son planteamientos a largo plazo, con consecuencias que pueden evolucionar mucho en función de cambios en el contexto social o tecnológico. El mantenimiento de los dispositivos y de los sistemas, la propiedad y responsabilidad de actualizar los mismos, así como el soporte al responsable para realizar toda la gestión de riesgos para los derechos y libertades (incluyendo la probable EIPD) son aspectos que se tienen que reflejar en dichos contratos.

Las AA.PP. deben de tomar conciencia de que cuanto mayor es la cantidad de información recogida y su frecuencia de obtención mayor será el riesgo inherente para la protección de datos de los ciudadanos. Estos tratamientos son inherentemente de alto

[187] Artículo 24 del RGPD – Responsabilidad del responsable del tratamiento
[188] Artículo 26 del RGPD – Corresponsables del tratamiento
[189] Artículo 28 del RGPD – Encargado del tratamiento
[190] Artículos 13 y 14 del RGPD – Información que deberá facilitarse cuando los datos personales se obtengan del interesado o cuando no se hayan obtenido del interesado, respectivamente.

riesgo[191] en la mayoría de los casos por la gran acumulación de datos que se realiza por parte de las AA.PP. .Por ello, la Guía para Administraciones locales[192] destaca la necesidad de que antes del despliegue de un proyecto 'Smart City' es necesario realizar:

- Un análisis previo del proyecto sobre el volumen de la información que se pretende procesar, el número y tipo de fuentes desde las que se pretende obtener dicha información, la frecuencia de recogida de datos y el tiempo durante el que se pretende conservar esta información.
- El análisis del enriquecimiento de datos, tanto planificado en el tratamiento como del riesgo de que este se produzca.
- Una evaluación de impacto en los términos establecidos en el artículo 35 del RGPD, valorando incluso la necesidad, según las características del proyecto, de elevar una consulta previa a la Autoridad de Protección de Datos

La gobernanza del sistema *Smart City* ha de integrar el cumplimiento que una política de protección de datos ha de tener previsto para corregir los problemas que se planteen. Además de los riesgos específicos de un tratamiento *Smart City*, ha de contemplarse gestionar los riesgos de las tecnologías involucradas.

Incluso cuando, en el proyecto *Smart City*, se recogen datos inicialmente anonimizados, la extensión, frecuencia, combinación y enriquecimiento de datos pueden resultar en una reidentificación de las personas. Todos tenemos unos hábitos de comportamiento que son únicos y revelan nuestro trabajo, con quién vivimos, nuestra salud o incluso nuestras convicciones políticas y religiosas. El riesgo de reidentificación se ha de evaluar y tomar medidas para mitigarlo, como puede ser aplicar técnicas de privacidad diferencial, empleo de estrategias de agregación de información para evitar correlaciones, recurrir al procesamiento local y distribuido para reducir la cantidad de datos almacenados de manera centralizada por un mismo responsable, etc.[193]

La instalación de sensores y actuadores de forma masiva incrementa la probabilidad de que se produzcan fallos de seguridad en los tres dominios: confidencialidad, disponibilidad e integridad por lo que un aspecto muy delicado a considerar es la seguridad ante posibles fallos y ante ataques intencionados[194]. Esta es la situación que se materializó de forma masiva en el año 2007 en la ciudad de Tallin[195]. El análisis de riesgos de seguridad desde el punto de vista de protección de datos ha de dar las máximas garantías para que no se puedan producir accesos no autorizados que permitan monitorizar personas singulares o un filtrado masivo de datos personales, uno de los grandes riesgos que tienen las *Smart City*.

La seguridad no puede ser total, pero sí se pueden poner en marcha planes preventivos de auditoría continua, como el hacking ético, análisis de cómo evolucionan los riesgos en función del contexto (por ejemplo, con el despliegue de nuevos servicios y tecnologías) y medidas que minimicen el impacto que una brecha puede tener, por muy improbable que ésta sea. Estas medidas pasan por la aplicación de criterios de minimización de datos, separación de datos en distintos sistemas, en el tiempo y en las categorías, ocultación de datos mediante técnicas de cifrado o seudonimización temprana o bloqueo de datos. En algunos casos podría ser interesante permitir al administrado tener control de la recogida

[191] Artículo 35.3.c) del RGPD – Evaluación de impacto relativa a la protección de datos (caso de observación sistemática a gran escala de una zona de acceso público)
[192] Guía para Administraciones Locales (AEPD): https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf
[193] Al igual que una referencia anterior: se recomienda consultar las publicaciones de la AEPD como: Orientaciones y garantías en los procedimientos de Anonimización de datos personales, la Introducción al hash como técnica de seudonimización de datos personales o La K-anonimidad como medida de privacidad.
[194] Smart Cities Cyber Security Worries. 2018 IOActive, Inc. Infografía en https://ioactive.com/wp-content/uploads/2018/10/IOActive-SmartCities-cybersecurity-worries.pdf
[195] Este evento llevó a una reacción de la OTAN: https://elpais.com/diario/2007/05/18/internacional/1179439204_850215.html

automática de sus datos, poniendo en marcha mecanismos autónomos y transparentes que contemplen la participación de los propios ciudadanos, de modo que estos puedan comprobar el cumplimiento efectivo de las garantías establecidas.

Existen dos momentos críticos que pueden suponer un mayor riesgo para los derechos y libertades: el momento de despliegue y el momento de retirada del sistema. El primero supone que el sistema no estará ajustado, en particular con relación a los riesgos de protección de datos, por lo que es conveniente que los despliegues sean limitados y que se solicite el consejo de las autoridades de control. El segundo es en el momento de la retirada o sustitución del sistema completo, ya que un sistema abandonado, o semi abandonado, puede resultar en una vulnerabilidad añadida.

IX. CONCLUSIONES

La transformación digital de las AA.PP. es una realidad fruto del uso intensivo de las nuevas tecnologías, algunas de ellas punteras, que persigue mejorar tanto su propia operativa interna como aumentar la calidad de servicio a los ciudadanos. Las posibilidades que ofrecen en diferentes sectores como la salud, la educación o la investigación son infinitas y no cabe que es un elemento clave para la mejora en la eficacia y eficiencia en la prestación de los servicios públicos.

Independientemente que todos los servicios implementados en las AA.PP. están guiados por un espíritu de servicio público, el tratamiento de datos personales en el seno de estas organizaciones tiene un riesgo característico y que se deriva del volumen de sujetos afectados, de la extensión de los datos recogidos, de la imposibilidad, en muchos casos, de oponerse al tratamiento y del desequilibrio existente entre Administración y ciudadanos.

Los riesgos inherentes se pueden materializar sobre los interesados en situaciones de quiebras del estado de derecho, de abuso por parte de los responsables públicos, filtrado masivo o selectivo de datos personales, brechas de seguridad, cambios legislativos incluso en terceros países, corrupción, emergencias fuera de control, etc.

El derecho fundamental a la protección de datos tuvo su origen en la necesidad de prevenir y evitar que se repitiesen los excesos trágicos que se produjeron en el siglo XX y que se fundamentaron en el tratamiento extenso[196], intrusivo[197] y, en algunos casos con cierto grado de automatización[198], de datos de carácter personal, incluso, a pesar del esfuerzo de empleados públicos que lucharon contra un sistema que ya les superaba[199].

En este sentido, hay que recordar que la normativa de protección de datos es un instrumento que, además de proteger los derechos y libertades de los ciudadanos, permite que tecnologías emergentes en la sociedad puedan emplearse también en las AA.PP. de forma sostenible y en línea con las políticas de responsabilidad social de las instituciones.

La normativa de protección de datos en Europa y en España es moderna y está bien alineada con las buenas prácticas de la ingeniería y de la gestión de proyectos actual. Esto es, básicamente, un enfoque proactivo adelantándose a los problemas y destacando la responsabilidad de los actores; y una gestión continua del riesgo, evitándolo, detectándolo de forma temprana y planificando su respuesta. En este sentido, puede decirse que cumplir la ley y hacer las cosas con sentido común van de la mano.

La tecnología está cambiando el mundo y es importante diseñar tratamientos que garanticen que ese cambio sea a mejor, al menos en el respeto a los derechos y libertades de las personas. Introducir la tecnología en los procesos tradicionales de las AA.PP., o implementar procesos nuevos en base a ella, cada vez es más sencillo, pero no por ello debe ser más arriesgado, intrusivo o incontrolado[200]. Al contrario, la creación de nuevos servicios en una sociedad en constante desarrollo, tanto a nivel social como tecnológico, introduce una mayor exposición al riesgo que requiere ser analizada y gestionada de forma individualizada en cada caso y condiciona a que los responsables de los tratamientos se

[196] Los registros civiles holandeses en 1940 contenían información sobre la religión de los ciudadanos y cayeron intactos en manos alemanas: https://en.wikipedia.org/wiki/History_of_the_Jews_in_the_Netherlands#The_Holocaust https://en.wikipedia.org/wiki/1943_bombing_of_the_Amsterdam_civil_registry_office

[197] Datos recopilados por los servicios de la RDA: https://elpais.com/diario/1991/10/07/internacional/686790013_850215.html

[198] IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation. Editor: Dialog Press 2012 ISBN-13: 978-0914153276

[199] Breve reseña de René Carmille: https://hipertextual.com/2018/12/rene-carmille-hombre-que-hackeo-nazis-ii-guerra-mundial

[200] A pesar de su antigüedad en muchos casos el llamado triángulo de hierro o triángulo de la gestión de proyectos sigue manteniendo su vigencia. La frase 'bueno, rápido o barato: elija dos' se ha hecho famosa en muchos ámbitos. https://en.wikipedia.org/wiki/Project_management_triangle .

planteen mejor las consecuencias derivadas de estos teniendo en cuenta que las cosas no siempre funcionan como se espera.

Los responsables públicos deben tener en mente además un factor adicional, y es que las tecnologías no están al alcance de todos los ciudadanos[201]. Y no solamente estamos pensando en las redes de comunicaciones, los ordenadores o las tabletas. Muchas personas, porque se educaron en otra época, por sus limitaciones o simplemente porque no han tenido curiosidad o tiempo para informarse, no entienden de tecnología. Puede que se cumplan todos los requisitos legales para informarles de qué se va a hacer con sus datos, pero eso no es suficiente: es preciso introducir garantías para explicarles las cosas de forma que se entiendan.

Ninguno de nosotros podemos proteger un bien si no sabemos que lo tenemos, que tiene un valor o que su pérdida o mal uso nos puede causar un perjuicio. Es una responsabilidad de las AA.PP., pero también de todos los responsables de los tratamientos, informar a sus usuarios de por qué deben ser cuidadosos con sus datos, cómo van a ser utilizados y qué van a ganar si nos dejan usarlos[202].

En este documento se han analizado un conjunto de tecnologías, más o menos punteras, señalando algunos de los riesgos que las AA.PP., como responsables, deben tener en cuenta cuando las incorporen como apoyo y soporte a los tratamientos que realizan. Es importante señalar al lector que este análisis no es completo ni exhaustivo tanto desde el punto de vista de la posible relación de riesgos como del abanico de tecnologías contempladas ya que ha pretendido servir de muestra del ejercicio reflexivo que los responsables del tratamiento deben realizar cuando se decidan a utilizar una nueva solución como parte de su proceso de transformación digital en el ámbito del desarrollo de sus competencias: análisis de la idoneidad, necesidad y de la proporcionalidad de su empleo, identificación de los riesgos que introduce, evaluación de impacto para la protección de datos que representa su utilización y obstáculos que puede representar en el cumplimiento de otras obligaciones marcadas por la normativa de protección de datos.

Una gestión proactiva del riesgo en materia de protección de datos por parte de las Administraciones junto con la adopción de criterios adecuados de transparencia, proporcionalidad, minimización y limitación del tratamiento actúan como factores determinantes para garantizar y promover la confianza de los ciudadanos en los servicios prestados.

[201] La brecha digital es cualquier distribución desigual en el acceso, en el uso, o en el impacto de las Tecnologías de la Información y la Comunicación (TIC) entre grupos sociales. Estos grupos pueden definirse con base en criterios de género, geográficos o geopolíticos, culturales, o de otro tipo. https://en.wikipedia.org/wiki/Digital_divide

[202] El barómetro del CIS de mayo de 2018 preguntaba a los encuestados sobre La protección de datos personales y el posible uso de información personal por otras personas (pregunta 9). A un 37,3% le preocupaba mucho, y a un 38,8% bastante. (http://datos.cis.es/pdf/Es3213mar_A.pdf)

X. ANEXOS

A. REFERENCIAS Y RECURSOS ÚTILES

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 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).

  https://www.boe.es/doue/2016/119/L00001-00088.pdf

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

  https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

- Guía de privacidad desde el diseño

  Agencia Española de Protección de Datos, octubre 2019

  https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

- Guía de protección de datos por diseño

  Agencia Española de Protección de Datos, octubre 2020

  https://www.aepd.es/media/guias/guia-proteccion-datos-por-defecto.pdf

- Guía para la gestión de brechas de seguridad

  Agencia Española de Protección de Datos, junio 2018

  https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

- Guía práctica de análisis de riesgos para el tratamiento de datos personales

  Agencia Española de Protección de Datos, febrero 2018

  https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf

- Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD

  Agencia Española de Protección de Datos, octubre 2018

  https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

- Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para las Administraciones Públicas

  Agencia Española de Protección de Datos,

  https://www.aepd.es/sites/default/files/2020-03/modelo-informe-EIPD-AAPP.rtf

- Listas de tipos de tratamientos de datos que requieren EIPD (art 35.4)

  Agencia Española de Protección de Datos, septiembre 2019

  https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

- Lista orientativa de tipos de tratamientos de datos que no requieren una evaluación de impacto relativa a la protección de datos (art 35.5)

  Agencia Española de Protección de Datos, agosto 2019

  https://www.aepd.es/sites/default/files/2019-09/ListasDPIA-35.5l.pdf

- Guía sobre el uso de las cookies

  Agencia Española de Protección de Datos, julio 2020

  https://www.aepd.es/media/guias/guia-cookies.pdf

- Estudio Fingerprinting o Huella digital del dispositivo

  Agencia Española de Protección de Datos, febrero 2019

  https://www.aepd.es/sites/default/files/2019-09/estudio-fingerprinting-huella-digital.pdf

- Informe sobre políticas de privacidad en internet

  Agencia Española de Protección de Datos, octubre 2018

  https://www.aepd.es/sites/default/files/2019-12/informe-politicas-de-privacidad-adaptacion-RGPD.pdf

- Decálogo para la adaptación al RGPD de las políticas de privacidad en internet

  Agencia Española de Protección de Datos, octubre 2018

  https://www.aepd.es/sites/default/files/2019-09/decalogo-politicas-de-privacidad-adaptacion-RGPD.pdf

- Guía para el cumplimiento del deber de informar

  Agencia Española de Protección de Datos; Autoridad Catalana de Protección de Datos, Agencia Vasca de Protección de Datos, enero 2017

  https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf

- Adecuación al RGPD de los tratamientos que incorporan Inteligencia Artificial. Una introducción.

  Agencia Española de Protección de Datos, febrero 2020

  https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

- Blockchain and the General Data Protection Regulation.

  European Parliamentary Research Service, EPRS, julio 2019

  https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

- Guía de protección de datos y Administración Local

  Agencia Española de Protección de Datos, abril 2018

  https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf

- Guía para clientes que contraten servicios de Cloud Computing

  Agencia Española de Protección de Datos, septiembre 2018

  https://www.aepd.es/sites/default/files/2019-09/guia-cloud-clientes.pdf

- Orientaciones para prestadores de servicios de Cloud Computing

  Agencia Española de Protección de Datos, septiembre 2018

  https://www.aepd.es/sites/default/files/2019-09/guia-cloud-prestadores.pdf

- Código de buenas prácticas en protección de datos para proyectos Big Data

  Agencia Española de Protección de Datos, mayo 2017
  https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

- Orientaciones y garantías en los procedimientos de Anonimización de datos personales

Agencia Española de Protección de Datos, 2016

https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf

- Dictamen 05/2014 sobre técnicas de anonimización

  Grupo de Trabajo sobre protección de datos del artículo 29, abril 2014

  https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdff

- Introducción al hash como técnica de seudonimización de datos personales

  Agencia Española de Protección de Datos, noviembre 2019

  https://www.aepd.es/sites/default/files/2019-11/estudio-hash-anonimidad.pdf

- La K-anonimidad como medida de privacidad

  Agencia Española de Protección de Datos, junio 2019

  https://www.aepd.es/sites/default/files/2019-09/nota-tecnica-kanonimidad.pdf

Puede acceder a más recursos y enlaces de interés a documentos y material de carácter tecnológico en el área de Innovación y Tecnología de la página web de la Agencia Española de Protección de Datos.

B. CONTACTO CON LAS AUTORIDADES DE PROTECCIÓN DE DATOS

La Agencia Española de Protección de Datos es la autoridad administrativa independiente de ámbito estatal a la que le corresponde supervisar la aplicación de la LOPDGDD y del RGPD. Además, las Comunidades Autónomas de Andalucía, Cataluña y País Vasco cuentan también con autoridades autonómicas de protección de datos que pueden ejercer las funciones y potestades atribuidas por el Reglamento a las autoridades de control, en los supuestos previstos en el artículo 57.1 de la LOPDGDD, a saber:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

De acuerdo con todo lo anterior, con carácter general, las AA.PP. deben notificar las brechas de seguridad a la AEPD a través del canal habilitado en la sede electrónica. Sin embargo, en el caso de Andalucía, Cataluña y País Vasco, cuando las brechas de seguridad se produzcan en los supuestos señalados anteriormente, la autoridad de control competente será la de la correspondiente Comunidad Autónoma, es decir:

- En el caso de Andalucía: el Consejo de Transparencia y Protección de Datos de Andalucía a través de su ventanilla electrónica
- En el caso de Cataluña: la Autoridad Catalana de Protección de Datos (https://apdcat.gencat.cat/es/inici/) a través de su sede electrónica.
- En el caso del País Vasco: la Agencia Vasca de Protección de Datos mediante el correo electrónico avpd@avpd.eus