Cuestións prácticas para a directa aplicación da normativa de protección de datos nas administracións públicas

Cuestiones prácticas para la directa aplicación de la normativa de protección de datos en las administraciones públicas

Between theory and practice, the data protection regulation in public administrations

57 Regap

LUCÍA DO NASCIMENTO LÓPEZ

Abogada especializada en Derecho de las Telecomunicaciones, Protección de Datos, Sociedad de la Información y Audiovisual
luciadonascimento@outlook.es

Recibido: 25/06/2019 | Aceptado: 18/07/2019

DOI: https://doi.org/10.36402/regap.v1i57.25

Resumo: Análise dos dereitos e obrigas relativos ás implicacións derivadas da normativa europea e nacional en materia de protección de datos respecto dos tratamentos realizados por parte das administracións públicas
Palabras clave: RGPD, Administración pública, LOPDGDD.

Resumen: Análisis de los derechos y obligaciones relativos a las implicaciones derivadas de la normativa europea y nacional en materia de protección de datos respecto de los tratamientos realizados por parte de las administraciones públicas
Palabras clave: RGPD, Administración pública, LOPDGDD.

Abstract: Analysis of the rights and obligations relating to the implications arising from European and national legislation on data protection with regard to the processing carried out by public administrations.
Key words: GDPR, public Administration, LOPDGDD.

1 Introducción

Con la entrada en aplicación, el pasado 25 de mayo, del 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 derogó la Directiva 95/46/CE (en adelante, RGPD), así como por la posterior aprobación de la Ley 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD), las administraciones públicas se han sometido a un intenso procedimiento de adaptación a dichas normas, puesto que estas, a partir de ese momento, se encuentran sometidas al cumplimiento de una serie de obligaciones que persiguen que el ingente número de datos de carácter personal tratados por dichos entes públicos en el ejercicio de sus funciones sea recubierto como si de una película se tratara, por una serie de medidas de índole jurídica, técnica y organizativa cuya finalidad no es otra que aseverar y garantizar la seguridad de dichos datos personales.

Por lo tanto, a continuación se exponen los requisitos que toda entidad pública debe contemplar dentro de su organización para que los tratamientos de datos de carácter personal se adecuen y, por lo tanto, cumplan de manera estricta con las disposiciones vigentes. No obstante, no debe olvidarse que el derecho a la protección de datos no es un derecho con carácter absoluto, sino que convive junto con otros derechos fundamentales, implicando tal situación la necesidad de alcanzar una armonía jurídica cuyo objetivo no es otro que respetar, de manera conjunta, entre otros, el derecho a la protección de datos, el derecho a la vida privada y familiar, el derecho relativo al secreto de las comunicaciones, el derecho de libertad de expresión e información, de conciencia y religión[1].

2 Bases de legitimación: eje fundamental para el correcto tratamiento de datos de carácter personal por parte de la Administración pública

Tal y como se ha mencionado, los tratamientos de datos de carácter personal que realizan las administraciones públicas deben ajustarse a las exigencias que contempla la norma nacional, lo que ha supuesto y supone un largo proceso de transformación debido al gran volumen de datos tratados, y todo ello de cara a la correcta prestación de los servicios públicos encomendados. A tal efecto, debe partirse de la necesidad de adecuar los tratamientos efectuados a las bases legitimadoras ofrecidas, puesto que este será el punto a partir del cual se podrán realizar lícitamente las actividades de tratamiento pretendidas sobre los datos personales de los ciudadanos, y también será necesario establecer una serie de procedimientos encaminados a garantizar la correcta conservación y seguridad de estos, con el ánimo de mitigar los posibles

[1] *Vid.* Considerando 4 del RGPD.

riesgos que se puedan producir dentro de la entidad para que todo ello pueda ser, tal y como se ha venido denominando en el último tiempo, *Compliance*[2].

Al hilo de lo anterior, la primera base legitimadora que se debe analizar es el consentimiento, puesto que este ha implicado un sustancial cambio a la hora de ser configurado, ya que debe ser facilitado por el afectado para las operaciones de tratamiento de sus datos en relación con uno o varios fines específicos.

Cabe destacar el importante valor que el texto europeo otorgó al consentimiento, dado que suprimió de manera absoluta el consentimiento tácito, lo que ha contribuido a que el titular de los datos tenga pleno conocimiento del tratamiento que sobre ellos se realiza, implicando la necesidad de que este "*debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca*"[3]. Así las cosas, la aceptación del tratamiento en cuestión podrá ser avalado, por ejemplo, a través de una declaración por escrito que podrá ser efectuada a través de medios electrónicos o bien mediante una declaración verbal, debiendo quedar acreditado –en ambos casos– que se ha cumplido con el deber de información exigido por la normativa, y tendrá que constar prueba plena del otorgamiento de dicho consentimiento.

En relación con lo anterior, será la Administración pública, como responsable del tratamiento, quien tendrá la obligación de demostrar que el consentimiento se ha recabado respetando las garantías recogidas en la normativa vigente en materia de protección de datos[4]. Por último, el legislador europeo, en aras a garantizar que el consentimiento facilitado por los titulares se fundamente en que este se ha prestado de forma libre, hace referencia a la imposibilidad de que el mismo se configure como fundamento jurídico válido en aquellos supuestos en los que se produzca un evidente desequilibrio entre el responsable del tratamiento y el afectado por el tratamiento de sus datos de carácter personal. Por ello, dicha base jurídica no será empleada con asiduidad, derivándose tal efecto de la significativa posición que alcanza el ente público frente al ciudadano.

Por consiguiente, esto ha supuesto, y así lo ha manifestado la Agencia Española de Protección de Datos (en adelante, AEPD), que la Administración pública, a la hora de configurar las bases legitimadoras que rigen las actividades de tratamiento desempeñadas, haga que se asienten principalmente en los dos fundamentos jurídicos que se señalan a continuación.

a) *El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.*

---

2 Rfc. WORLD COMPLIANCE ASSOCIATION define el *Corporate Compliance* como el conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer así mecanismos internos de prevención, gestión, control y reacción frente a estos.

3 *Vid.* Considerando 42 del RGPD.

4 De acuerdo con la Directiva 93/13/CEE del Consejo (1), debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

b) *El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*.

A tal efecto, para llevar a cabo la correcta aplicación de estos, debe atenderse a lo establecido en el artículo 8 de la LOPDGDD, el cual, en síntesis, viene a indicar que:

1. Para poder fundamentar el tratamiento en el cumplimiento de una obligación legal exigible al responsable, será necesario que dicha actividad se encuentre determinada por una norma de derecho de la Unión Europea o una norma con rango de ley.

2. Para que pueda ser aplicada la base legitimadora consistente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, será requisito esencial que dicho tratamiento sea consecuencia de la competencia que la Administración pública tiene conferida a través de una norma con rango de ley.

En este punto, resulta interesante resaltar la modificación que se ha llevado a cabo respecto a los puntos 2 y 3 del artículo 28 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, la cual ha trasladado el consentimiento para la consulta u obtención de documentos elaborados por cualquier Administración, en relación con la aportación de documentos de carácter preceptivo o facultativo, a la base fundada en el cumplimiento de una misión realizada en interés público, permitiendo al afectado ejercitar, en todo momento, su derecho de oposición al tratamiento.

La misma circunstancia se ha producido respecto al requerimiento, por parte de las administraciones públicas, de documentos presentados con anterioridad a cualquier Administración, capacitando a esta para su recabado, salvo que conste oposición expresa del interesado o, en su caso, por la aplicación de una ley especial, sea requerido el consentimiento expreso del titular de los datos.

Unido a lo anterior, se concede la potestad a las administraciones públicas, por medio de la disposición adicional octava de la LOPDGDD, de verificar la exactitud de los datos de carácter personal de los afectados, cuando por cualquier medio estos formulen solicitudes en las que el ciudadano declare datos personales que obren en poder de dichos entes.

Conforme cuanto antecede, debe matizarse que no todos los tratamientos que se realicen por parte de las administraciones públicas estarán amparados en el artículo 8.2 de la antedicha norma, sino que, y así lo ha expuesto la AEPD por medio del Informe 2018-175, emitido por su Gabinete Jurídico, "*Si un determinado tratamiento no es «necesario» para el cumplimiento de la misión realizada en interés público o en el ejercicio de los poderes públicos conferidos por el ordenamiento, dicho tratamiento no solo carecería de base jurídica suficiente legitimadora prevista en el apartado e), sino que, además, infringiría el principio de minimización de datos contenido en el artículo 5.1.c) RGPD, aplicable igualmente a los tratamientos de datos llevados a cabo por la Administración pública*"[5].

En consecuencia, la aplicación de la condición que establece que el tratamiento será lícito si este es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, se verá excluida del ámbito de

[5] *Vid.* www.aepd.es/media/informes/2018-0175-base-juridica-tratamiento-por-la-administracion-publica.pdf

aplicación la Administración pública, puesto que, en relación con lo referido, primará la aplicación del fundamento basado en el cumplimiento de una obligación legal o, en su caso, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. Igualmente, dicho posicionamiento se deriva de lo establecido por el considerando 45 del RGPD[6].

No obstante, resulta preciso analizar la capacidad que tendrán tales entidades cuando, encontrándose al margen de sus funciones públicas, es decir, cuando actúe como un sujeto de derecho privado, pueda aplicar el interés legítimo como eje del tratamiento de datos de carácter personal. A tal efecto, es necesario traer a colación la sentencia emitida por el Tribunal de Justicia de la Unión Europea, Sala Segunda, el 19 de octubre de 2016. En el asunto C 852/14 (*Patrick Breyer y Bundesrepublik Deutschland*) apartados 53 y 60 –dictada en interpretación del concepto de interés legítimo del artículo 7.1.f) de la Directiva 95/46 y, por tanto, anterior al RGPD– admite que una autoridad pública puede tener un interés legítimo como base jurídica en sus tratamientos de datos[7].

53. Pues bien, en el asunto principal, sin perjuicio de las comprobaciones que debe realizar a este respecto el tribunal remitente, parece que los organismos federales alemanes que prestan servicios de medios en línea y que son responsables del tratamiento de las direcciones IP dinámicas actúan, a pesar de su estatuto de autoridades públicas, en calidad de particulares y fuera del ámbito de las actividades del Estado en materia penal.

60. (...) Pues bien, los organismos federales alemanes que suministran servicios de medios en línea podrían tener también un interés legítimo en garantizar, más allá de cada utilización concreta de sus sitios de Internet accesibles al público, la continuidad del funcionamiento de dichos sitios.

En relación con esta cuestión, la AEPD, con base en los criterios emitidos por parte del Grupo de Trabajo del Artículo 29 (en adelante, GT29), a través del Dictamen 06/2014, se ha posicionado indicando que se considera pertinente dejar a un lado el interés legítimo, independientemente de que las funciones que se desempeñen se sometan a actividades relacionadas con derecho privado, puesto que tales actividades podrán ser encuadradas en el marco del cumplimiento de una misión realizada en interés público. No obstante, dicho criterio no es mantenido, por ejemplo, por parte de la autoridad de control británica (ICO), que considera que los entes públicos tienen

6 Considerando 45 del RGPD. "*Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional*".

7 *Vid.* http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=ES.

legitimación para aplicar y, en consecuencia, desarrollar actividades del tratamiento sobre la base del interés legítimo.

Por último, será lícito el tratamiento llevado a cabo si este es necesario para proteger los intereses vitales del interesado o de otra persona física.

A la luz de lo expuesto, ha quedado patente la importancia de analizar y, en consecuencia, aplicar los fundamentos jurídicos adecuados al caso concreto, y todo ello sin perder de vista el deber de información al que todo responsable del tratamiento se encuentra sujeto.

3 Regulación de los contratos de acceso a datos

Asentado lo anterior, el cambio normativo ha supuesto un importante esfuerzo a la hora de adecuar toda la documentación por medio de la cual se recababan datos de carácter personal del ciudadano, así como todos aquellos otros documentos que hacen referencia a tratamientos de datos de carácter personal que afecten al funcionariado público o cualquier otro empleado contratado en el seno de la organización.

Directamente, esto ha conllevado a la revisión directa y actualización de los contratos suscritos con los encargados del tratamiento, sujetos que llevan a cabo los tratamientos por cuenta del responsable y que deberán cumplir igualmente con las disposiciones europeas y nacionales en materia de protección de datos.

A pesar de que es recomendable efectuar una revisión de los contratos de acceso a datos, la LOPDGDD, por medio de su disposición transitoria quinta, estableció que los contratos perfeccionados con anterioridad al 25 de mayo de 2018, es decir, antes de la aplicación del RGPD, mantendrán su vigencia hasta la fecha de su vencimiento y, en el caso de que tengan carácter indefinido, su actualización se podrá prorrogar hasta el 25 de mayo de 2022.

Asimismo, las administraciones públicas tendrán la obligación de cerciorarse de que los encargados del tratamiento seleccionados ofrecen garantías suficientes para aplicar medidas de índole técnica y organizativa apropiadas y, en consecuencia, que estas aseguren la protección de los datos personales tratados conforme a los preceptos recogidos en la normativa, garantizando así la tutela de los derechos de los afectados.

En esta línea, cobran vital interés las directrices establecidas por parte de las administraciones públicas a través de los contratos de acceso a datos perfeccionados, puesto que mediante la configuración de estos se derivarán las pertinentes responsabilidades generadas como resultado de un incumplimiento contractual o, en su caso, de un fallo de seguridad. Por tanto, debe hacerse especial hincapié en las estipulaciones que hacen referencia a la facultad del encargado del tratamiento para destinar los datos a finalidades diferentes para las cuales se han facilitado, la posibilidad de comunicar esos datos a terceros, es decir, llevar a cabo cesiones de datos, así como acudir a terceros para la prestación de determinados servicios y la manera de proceder en caso de que tenga lugar tal situación, siéndole de aplicación a este último encargado las mismas obligaciones que las que le fueron impuestas al

encargado inicial. Tales obligaciones serán exigidas a través de un contrato u otro acto jurídico establecido con arreglo al derecho de la Unión o de los Estados miembros.

De igual modo, tendrán que seguirse las instrucciones dadas por la Administración pública, como responsable del tratamiento, para poder llevar a cabo las transferencias internacionales de datos de carácter personal (en adelante, TID), situación que se produce cuando estos se remiten fuera del ámbito del Espacio Económico Europeo[8]. A tal efecto, no solamente deberá prestarse atención a las TID que tengan su origen en la propia actividad de la Administración, sino que será especialmente relevante controlar y regular todas aquellas TID que se originan como corolario de la evolución de las tecnologías de la información y comunicación, así como del uso, cada vez más recurrente, de los servicios en nube (*cloud computing*)[9]. En este extremo, cabe destacar que el texto europeo acrecienta los instrumentos a través de los cuales se podrán realizar estas transferencias, entre los que se incorporan los jurídicamente requeridos y vinculantes entre autoridades y organismos públicos[10].

A su vez, será fundamental establecer en dichos contratos el modo de proceder del encargado del tratamiento cuando se produzca una brecha o violación de seguridad de los datos personales, es decir, cuando se "*ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*"[11].

En estos supuestos, será indispensable establecer el plazo para la comunicación de dichas brechas de seguridad, el cual podrá ser superior a 24 horas, siendo recomendable que, a la hora de perfeccionar dicho plazo en el contrato, este preferiblemente no supere las 48 horas, puesto que será el responsable del tratamiento quien tendrá que notificar a la autoridad de control competente tal acontecimiento, sin dilación indebida y, a más tardar, dentro de las 72 horas siguientes[12] desde que se haya producido la brecha de seguridad, siempre y cuando esta constituya un riesgo para los derechos y libertades de los afectados.

Esto conllevará que, para la minimización de los riesgos que se quieran asumir por medio del contrato, el encargado del tratamiento facilite la información que a

8 Rfc. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Protección de Datos y Administración Local", *Guías Sectoriales AEPD*. Disponible en: https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf

9 Rfc. IBM Cloud. El *cloud computing* consiste en el suministro, bajo demanda, de recursos informáticos a través de internet y basado en un modelo de pago por uso.

10 *Vid.* art. 46 del RGPD.

11 *Vid.* art. 4 del RGPD.

12 El considerando 85 del RGPD establece que, "*Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida*".

continuación se detalla, en aras a realizar una adecuada y eficaz gestión, así como comunicación de los quebrantamientos acaecidos. Dicha información deberá contener los siguientes puntos[13]:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Por otro lado, ni la normativa internacional ni nacional ofrecen una lista exhaustiva de todas aquellas medidas de seguridad de carácter técnico y organizativo que deberán ser aplicadas en relación con los tratamientos efectuados. En este sentido, y tal y como se ha venido realizando hasta el momento, las administraciones públicas deberán aplicar todas las medidas contenidas en el Esquema Nacional de Seguridad (en adelante, ENS), el cual establece aquellas a las cuales conviene adherirse en relación con los tratamientos de datos de carácter personal efectuados.

En este punto, la disposición adicional primera de la LOPDGDG incorpora el deber que tienen los responsables del tratamiento para exigir a los encargados configurados como empresas o fundaciones sujetas a derecho privado la adopción, en el seno de su organización, de medidas equivalentes a las establecidas por el ENS. A su vez, este requisito será el aplicado en aquellos supuestos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, debiendo corresponderse las medidas aplicadas con las de la Administración pública de origen.

Con todo ello, se pretende alcanzar el cumplimiento de la protección de datos desde el diseño y por defecto[14], dos nuevos principios introducidos por el RGPD con el propósito de que todas las organizaciones e instituciones respeten y respalden la privacidad de la información de los titulares y, en consecuencia, cumplan con otro de los nuevos principios recogidos en el texto europeo, la responsabilidad proactiva –también conocido como *accountability*–.

En consecuencia, el responsable deberá documentar por medio de un registro de actividades del tratamiento aquellas efectuadas bajo su responsabilidad, que ha venido a sustituir la obligación de notificar los ficheros y tratamientos a las autoridades

[13] *Vid.* art. 33 del RGPD.

[14] Rfc. la AEPD en su Guía "*Protección de Datos y Administración Local*" recoge que el principio de protección de datos desde el diseño supone que la protección de datos ha de estar presente en las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo. Asimismo, entiende que la protección de datos por defecto estriba en que solo sean objeto de tratamiento los datos personales que sean estrictamente necesarios para cada uno de los fines de tratamiento.

de control de protección de datos[15]. Por su parte, el encargado del tratamiento tendrá la obligación de documentar en dicho registro las categorías de actividades efectuadas por cuenta del responsable. Así las cosas, el registro de actividades del tratamiento tendrá que mantenerse actualizado, ya que se trata de un documento vivo, debiendo encontrarse, en todo momento, a disposición de las autoridades de control[16].

Una vez documentadas dichas actividades, será necesario realizar un análisis de los riesgos que estas comportan –englobando tanto las ya existentes como las que vayan a tener lugar–, para determinar si es pertinente realizar o no una evaluación de impacto sobre la protección de datos (en adelante, EIPD). En este sentido, las administraciones públicas españolas cuentan actualmente con metodologías de análisis y gestión de riesgos, principalmente en el ámbito de los sistemas de la información, como, por ejemplo, la norma *ISO 27005*, que derogó las normas *ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000*, o *MAGERIT*[17]. Esta última se constituye como una metodología de carácter público y se encuentra reconocida por ENISA[18], configurándose como un instrumento que pretende posibilitar la implantación y aplicación del ENS[19].

Asimismo, las EIPD deben ser realizadas con anterioridad a la puesta en marcha de los tratamientos y, cuando se considere que estos entrañan una serie de peligros para las libertades y derechos de los titulares, fijando a su vez una secuencia de supuestos en los que será preceptivo realizar dicha evaluación. Sin embargo, es cierto que el texto europeo exceptúa la necesidad de realizar una EIPD en tratamientos que no suponen un alto riesgo para los derechos y libertades de los titulares, siempre y cuando estos descansen sobre la base legitimadora relativa a la consecución de fines de interés público o se encuentren ligados al fundamento referente al ejercicio de los poderes públicos. Tal y como ha indicado la autoridad de control española, no se tendrán que someter a EIPD estos tratamientos, en los supuestos de que exista una

15 Rfc. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Públicas". Disponible en: https://www.aepd.es/media/docs/impacto-rgpd-en-aapp.pdf

16 Rfc. RODRÍGUEZ, B., "Cuáles son las exigencias de RGPD", *Revista Byte TI. Legalidad TIC*, 17 abril de 2018.

17 Rfc. PORTAL ADMINISTRACIÓN ELECTRÓNICA, GOBIERNO DE ESPAÑA. MAGERIT persigue estos objetivos: i) concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos, ii) ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicación (TIC), iii) ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control indirectos, iv) preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

18 La European Network and Information Security Agency (ENISA) es la Agencia de la Unión Europea para la Seguridad de las Redes y la Información, constituyéndose como un centro de experiencia para la ciberseguridad, con el que se pretende dotar a la UE y los países que la conforman de consejos prácticos y soluciones tanto al sector público como privado, para prevenir, detectar y responder a los problemas que se originen como consecuencia de la seguridad de la información.

19 CN-CERT. CENTRO CRIPTOLÓGICO NACIONAL. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos estableció el Esquema Nacional de Seguridad, que, aprobado mediante el Real decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación, y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, recoge el Esquema Nacional de Seguridad en su artículo 156, apartado 2, en similares términos. En 2015 se publicó la modificación del Esquema Nacional de Seguridad a través del Real decreto 951/2015, de 23 de octubre, en respuesta a la evolución del entorno regulatorio, en especial de la Unión Europea, de las tecnologías de la información y de la experiencia de la implantación del esquema.

norma que los regularice y se haya realizado una evaluación, como parte de una EIPD general, en el contexto de la adopción de esa norma de base[20].

No es cuestión baladí la importancia que radica en cuanto a la cooperación que debe existir entre los responsables y encargados del tratamiento, ya no solo respecto a las contingencias acaecidas en el marco de la prestación de servicios, sino también en cuanto a la correcta atención de los derechos de acceso, rectificación, oposición, supresión, limitación y portabilidad de los datos ejercitados por los titulares de los datos de carácter personal. Para el ejercicio de ellos, las administraciones públicas deberán habilitar mecanismos sencillos, accesibles y visibles para los ciudadanos, así como establecer procedimientos que impliquen la verificación de la identidad del titular en el supuesto de que se permita el ejercicio de tales derechos a través de medios electrónicos, como por ejemplo remitir una copia del documento nacional de identidad.

Retomando la importancia del deber de colaboración descrito, será determinante establecer el plazo que tiene el encargado del tratamiento para dar traslado al responsable de las solicitudes formuladas por los afectados por los tratamientos de sus datos de carácter personal, así como establecer la imposición de medidas adecuadas en aras a garantizar la correcta recepción de estas, en el caso de que no se atribuya la facultad de contestación a tales peticiones al encargado del tratamiento. Igualmente, estas cuestiones deberán ser reflejadas en el contrato suscrito entre ambas partes.

En cuanto a la figura del delegado de protección de datos, este se reviste de carácter obligatorio, cabiendo la posibilidad de nombrar un único delegado para varios organismos, si bien es cierto que tal decisión tendrá que atender al tamaño y estructura de dicha entidad pública. Asimismo, los delegados, tal y como indica el considerando 97 del RGPD, deberán poseer conocimientos especializados en derecho y la práctica en materia de protección de datos. Finalmente, tendrán que ser establecidas las unidades en las cuales este será integrado y la posición que tiene dentro del ente público, debiendo ser habilitados mecanismos que permitan a los ciudadanos contactar con él, como por ejemplo a través de la inclusión, dentro de la política de privacidad de la página web o en los formularios que se encuentren a disposición del público, de su correo electrónico.

Por último, todas las directrices que se han ido mencionando a lo largo de este estudio y que suponen, en definitiva, una exposición de los puntos más relevantes que afectan de un modo directo a la Administración pública y a los proveedores de servicios de las mismas deberán encontrarse sujetas al deber de secreto y confidencialidad.

Bibliografía

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), "Protección de Datos y Administración Local", *Guías Sectoriales AEPD*. Disponible en: https://www.aepd.es/media/guias/guia-proteccion-datos-administracion-local.pdf

[20] Rfc. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Públicas", cit.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "El impacto del Reglamento General de Protección de Datos sobre la actividad de las Administraciones Públicas". Disponible en: https://www.aepd.es/media/docs/impacto-rgpd-en-aapp.pdf

CAMPOS ACUÑA, M.ª C. (dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, Wolters Kluwer, Madrid, 2018.

CARRIÓN GARCÍA DE PARADA, F.J., y REGUERA GÓMEZ, M., "Reflexiones sobre la protección jurídica de las bases de datos. Auto del Tribunal Supremo de fecha 31 de enero de 2018", *Comunicaciones en propiedad industrial y derecho de la competencia*, n. 83 (enero-abril) 2018.

JIMÉNEZ ASENSIO, R., y MORO, A., *Manual-guía sobre impactos del Reglamento (UE) de protección de datos en los entes locales*, Federació de Municipis de Catalunya, 2018. Disponible en: https://www.fmc.cat/documents/25050/doc/Manual-Guia-castella.pdf

NÚÑEZ SEOANE, J., *Comunicación de datos personales por las Administraciones Públicas en el RGPD*, Blog Abogacía Española, 2018. Disponible en: https://www.abogacia.es/2018/07/17/comunicacion-de-datos-personales-por-las-administraciones-publicas-en-el-rgpd/

OROZ VALENCIA, L., "El día a día en las entidades locales y la influencia de la Ley Orgánica de Protección de Datos de carácter Personal", *Actualidad Administrativa*, n. 9, 2015.

POVEDANO ALONSO, D., "Comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en su aplicación a las entidades locales", *Actualidad Administrativa*, n. 1, 2019.

RODRIGUEZ, B., "Cuáles son las exigencias de RGPD", *Revista Byte TI. Legalidad TIC*, 17 abril de 2018.

TRONCOSO REIGADA, A., "La seguridad en el Reglamento General de Protección de Datos de la Unión Europea", *Actualidad Administrativa*, n. 1, 2019.

URGELL, E., "El RGPD: un cambio de paradigma en la protección de datos", *Revista Byte TI. Legalidad TIC*, mayo 2018.