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

Regap 57

LUCÍA DO NASCIMENTO LÓPEZ

Avogada especializada en Dereito das Telecomunicacións, Protección de Datos, Sociedade da Información e 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: RXPD, 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.

SUMARIO: 1 Introdución. 2 Bases de lexitimación: eixe fundamental para o correcto tratamento de datos de carácter persoal por parte da Administración pública. 3 Regulación dos contratos de acceso a datos.

1 Introdución

Coa entrada en aplicación, o pasado 25 de maio, do Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello do 27 de abril de 2016 relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e polo que se derrogou a Directiva 95/46/CE (en diante, RXPD), así como pola posterior aprobación da Lei 3/2018, do 5 de decembro, de protección de datos persoais e garantía dos dereitos dixitais (en diante, LOPDGDD), as administracións públicas sometéronse a un intenso procedemento de adaptación ás ditas normas, debido a que estas, a partir dese momento, se atopan sometidas ao cumprimento dunha serie de obrigas que perseguen que o inxente número de datos de carácter persoal tratados por eses entes públicos no exercicio das súas funcións sexa recuberto como se dunha película se tratase, por unha serie de medidas de índole xurídica, técnica e organizativa cuxa finalidade non é outra que aseverar e garantir a seguridade deses datos persoais.

Polo tanto, a continuación expóñense os requisitos que toda entidade pública debe contemplar dentro da súa organización para que os tratamentos de datos de carácter persoal se adecúen e, polo tanto, cumpran de xeito estrito coas disposicións vixentes. Non obstante, non se debe esquecer que o dereito á protección de datos non é un dereito con carácter absoluto, senón que convive xunto con outros dereitos fundamentais, implicando tal situación a necesidade de acadar unha harmonía xurídica cuxo obxectivo non é outro que respectar, de xeito conxunto, entre outros, o dereito á protección de datos, o dereito á vida privada e familiar, o dereito relativo ao segredo das comunicacións, o dereito de liberdade de expresión e información, de conciencia e relixión[1].

2 Bases de lexitimación: eixe fundamental para o correcto tratamento de datos de carácter persoal por parte da Administración pública

Tal como se mencionou, os tratamentos de datos de carácter persoal que realizan as administracións públicas deben axustarse ás exixencias que contempla a norma nacional, o que supuxo e supón un longo proceso de transformación debido ao gran volume de datos tratados, e todo iso de cara á correcta prestación dos servizos públicos encomendados. Para tal efecto, debe partirse da necesidade de adecuar os tratamentos efectuados ás bases lexitimadoras ofrecidas, posto que este será o punto a partir do cal se poderán realizar licitamente as actividades de tratamento pretendidas sobre os datos persoais dos cidadáns, e tamén será necesario establecer unha serie de procedementos encamiñados a garantir a correcta conservación e seguridade destes,

[1] *Vid.* Considerando 4 do RXPD.

co ánimo de mitigar os posibles riscos que se poidan producir dentro da entidade para que todo iso poida ser, tal como se veu denominando no último tempo, *Compliance*[2].

Ao fío do anterior, a primeira base lexitimadora que se debe analizar é o consentimento, dado que este implicou un substancial cambio á hora de ser configurado, xa que debe ser facilitado polo afectado para as operacións de tratamento dos seus datos en relación cun ou varios fins específicos.

Cabe destacar o importante valor que o texto europeo lle outorgou ao consentimento, pois suprimiu de xeito absoluto o consentimento tácito, o que contribuíu a que o titular dos datos teña pleno coñecemento do tratamento que sobre eles se realiza, implicando a necesidade de que este "*debe darse mediante un acto afirmativo claro que reflicta unha manifestación de vontade libre, específica, informada e inequívoca*"[3]. Así as cousas, a aceptación do tratamento en cuestión poderá ser avalado, por exemplo, a través dunha declaración por escrito que poderá ser efectuada a través de medios electrónicos ou ben mediante unha declaración verbal, debendo quedar acreditado –en ambos os dous casos– que se cumpriu co deber de información exixido pola normativa, e terá que constar proba plena do outorgamento do dito consentimento.

En relación co anterior, será a Administración pública, como responsable do tratamento, quen terá a obriga de demostrar que o consentimento se solicitou respectando as garantías recollidas na normativa vixente en materia de protección de datos[4]. Por último, o lexislador europeo, co fin de garantir que o consentimento facilitado polos titulares se fundamente en que este se prestou de forma libre, fai referencia á imposibilidade de que este se configure como fundamento xurídico válido naqueles supostos en que se produza un evidente desequilibrio entre o responsable do tratamento e o afectado polo tratamento dos seus datos de carácter persoal. Por iso, a dita base xurídica non será empregada con asiduidade, derivando tal efecto da significativa posición que alcanza o ente público fronte ao cidadán.

Por conseguinte, isto supuxo, e así o manifestou a Axencia Española de Protección de Datos (en diante, AEPD), que a Administración pública, á hora de configurar as bases lexitimadoras que rexen as actividades de tratamento desempeñadas, faga que se asenten principalmente nos dous fundamentos xurídicos que se sinalan deseguido.

a) *O tratamento é necesario para o cumprimento dunha obriga legal aplicable ao responsable do tratamento.*

b) *O tratamento é necesario para o cumprimento dunha misión realizada en interese público ou no exercicio de poderes públicos conferidos ao responsable do tratamento.*

---

2 Rfc. WORLD COMPLIANCE ASSOCIATION define o *Corporate Compliance* como o conxunto de procedementos e boas prácticas adoptados polas organizacións para identificar e clasificar os riscos operativos e legais a que se enfrontan e establecer así mecanismos internos de prevención, xestión, control e reacción fronte a estes.

3 *Vid.* Considerando 42 do RXPD.

4 De acordo coa Directiva 93/13/CEE do Consello (1), debe proporcionarse un modelo de declaración de consentimento elaborado previamente polo responsable do tratamento cunha formulación intelixible e de doado acceso que empregue unha linguaxe clara e sinxela, e que non conteña cláusulas abusivas. Para que o consentimento sexa informado, o interesado debe coñecer como mínimo a identidade do responsable do tratamento e os fins do tratamento aos cales están destinados os datos persoais. O consentimento non debe considerarse libremente prestado cando o interesado non goza de verdadeira ou libre elección ou non pode denegar ou retirar o seu consentimento sen sufrir prexuízo ningún.

Para tal efecto, para levar a cabo a correcta aplicación destes, debe atenderse ao establecido no artigo 8 da LOPDGDD, o cal, en síntese, indica que:

1. Para poder fundamentar o tratamento no cumprimento dunha obriga legal exixible ao responsable, será necesario que a dita actividade se atope determinada por unha norma de dereito da Unión Europea ou unha norma con rango de lei.

2. Para que poida ser aplicada a base lexitimadora consistente no cumprimento dunha misión realizada en interese público ou no exercicio de poderes públicos, será requisito esencial que ese tratamento sexa consecuencia da competencia que a Administración pública ten conferida a través dunha norma con rango de lei.

Neste punto, resulta interesante resaltar a modificación que se levou a cabo respecto aos puntos 2 e 3 do artigo 28 da Lei 39/2015, do 1 de outubro, do procedemento administrativo común das administracións públicas, a cal trasladou o consentimento para a consulta ou obtención de documentos elaborados por calquera Administración, en relación coa achega de documentos de carácter preceptivo ou facultativo, á base fundada no cumprimento dunha misión realizada en interese público, permitíndolle ao afectado exercer, en todo momento, o seu dereito de oposición ao tratamento.

A mesma circunstancia se produciu respecto ao requirimento, por parte das administracións públicas, de documentos presentados con anterioridade a calquera Administración, capacitando a esta para a súa recollida, salvo que conste oposición expresa do interesado ou, se é o caso, pola aplicación dunha lei especial, sexa requirido o consentimento expreso do titular dos datos.

Unido ao anterior, concédeselles a potestade ás administracións públicas, por medio da disposición adicional oitava da LOPDGDD, de verificar a exactitude dos datos de carácter persoal dos afectados, cando por calquera medio estes formulen solicitudes en que o cidadán declare datos persoais que consten en poder dos ditos entes.

Conforme canto antecede, debe matizarse que non todos os tratamentos que se realicen por parte das administracións públicas estarán amparados no artigo 8.2 da antedita norma, senón que, e así o expuxo a AEPD por medio do Informe 2018-175, emitido polo seu Gabinete Xurídico, "*Se un determinado tratamento non é necesario para o cumprimento da misión realizada en interese público ou no exercicio dos poderes públicos conferidos polo ordenamento, o dito tratamento non s*ó carecería de base xurídica suficiente *lexitimadora prevista no apartado e), senón que, ademais, infrinxiría o principio de minimización de datos contido no artigo 5.1.c) RXPD, aplicable igualmente aos tratamentos de datos levados a cabo pola Administración pública*"[5].

En consecuencia, a aplicación da condición que establece que o tratamento será lícito se este é necesario para a satisfacción de intereses lexítimos perseguidos polo responsable do tratamento ou por un terceiro, verase excluída do ámbito de aplicación a Administración pública, posto que, en relación co referido, primará a aplicación do fundamento baseado no cumprimento dunha obriga legal ou, se é o caso, cumprimento dunha misión realizada en interese público ou no exercicio de poderes

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

públicos. Igualmente, o dito posicionamento deriva do establecido polo considerando 45 do RXPD[6].

Non obstante, resulta preciso analizar a capacidade que terán tales entidades cando, atopándose á marxe das súas funcións públicas, é dicir, cando actúe como un suxeito de dereito privado, poida aplicar o interese lexítimo como eixe do tratamento de datos de carácter persoal. Para tal efecto, cómpre traer a colación a sentenza emitida polo Tribunal de Xustiza da Unión Europea, Sala Segunda, o 19 de outubro de 2016. No asunto C 852/14 (*Patrick Breyer e Bundesrepublik Deutschland*) apartados 53 e 60 –ditada en interpretación do concepto de interese lexítimo do artigo 7.1.f) da Directiva 95/46 e, polo tanto, anterior ao RXPD– admite que unha autoridade pública pode ter un interese lexítimo como base xurídica nos seus tratamentos de datos[7].

53. Pois ben, no asunto principal, sen prexuízo das comprobacións que debe realizar a este respecto o tribunal remitente, parece que os organismos federais alemáns que prestan servizos de medios en liña e que son responsables do tratamento dos enderezos IP dinámicos actúan, malia o seu estatuto de autoridades públicas, en calidade de particulares e fóra do ámbito das actividades do Estado en materia penal.

60. (...) Pois ben, os organismos federais alemáns que subministran servizos de medios en liña poderían ter tamén un interese lexítimo en garantir, máis alá de cada utilización concreta dos seus sitios de Internet accesibles ao público, a continuidade do funcionamento dos ditos sitios.

En relación con esta cuestión, a AEPD, con base nos criterios emitidos por parte do Grupo de Traballo do Artigo 29 (en diante, GT29), a través do Ditame 06/2014, posicionouse indicando que se considera pertinente deixar a un lado o interese lexítimo, independentemente de que as funcións que se desempeñen se sometan a actividades relacionadas con dereito privado, posto que tales actividades poderán ser encadradas no marco do cumprimento dunha misión realizada en interese público. No entanto, o dito criterio non é mantido, por exemplo, por parte da autoridade de control británica (ICO), que considera que os entes públicos teñen lexitimación para aplicar e, en consecuencia, desenvolver actividades do tratamento sobre a base do interese lexítimo.

Por último, será lícito o tratamento levado a cabo se este é necesario para protexer os intereses vitais do interesado ou doutra persoa física.

---

[6] Considerando 45 do RXPD. "*Cando se realice en cumprimento dunha obriga legal aplicable ao responsable do tratamento, ou se é necesario para o cumprimento dunha misión realizada en interese público ou no exercicio de poderes públicos, o tratamento debe ter unha base no dereito da Unión ou dos Estados membros. Este regulamento non require que cada tratamento individual se rexa por unha norma específica. Unha norma pode ser suficiente como base para varias operacións de tratamento de datos baseadas nunha obriga legal aplicable ao responsable do tratamento, ou se o tratamento é necesario para o cumprimento dunha misión realizada en interese público ou no exercicio de poderes públicos. A finalidade do tratamento tamén debe determinase en virtude do dereito da Unión ou dos Estados membros. Ademais, a dita norma podería especificar as condicións xerais deste regulamento polas que se rexe a licitude do tratamento de datos persoais, establecer especificacións para a determinación do responsable do tratamento, o tipo de datos persoais obxecto de tratamento, os interesados afectados, as entidades ás que se lles poden comunicar os datos persoais, as limitacións da finalidade, o prazo de conservación dos datos e outras medidas para garantir un tratamento lícito e leal. Debe determinarse tamén en virtude do dereito da Unión ou dos Estados membros se o responsable do tratamento que realiza unha misión en interese público ou no exercicio de poderes públicos debe ser unha autoridade pública ou outra persoa física ou xurídica de dereito público, ou, cando se faga en interese público, incluídos fins sanitarios como a saúde pública, a protección social e a xestión dos servizos de sanidade, de dereito privado, como unha asociación profesional*".

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

Á luz do exposto, quedou patente a importancia de analizar e, en consecuencia, aplicar os fundamentos xurídicos axeitados ao caso concreto, e todo iso sen perder de vista o deber de información a que todo responsable do tratamento se atopa suxeito.

3 Regulación dos contratos de acceso a datos

Asentado o anterior, o cambio normativo supuxo un importante esforzo á hora de adecuar toda a documentación por medio da cal se solicitaban datos de carácter persoal do cidadán, así como todos aqueloutros documentos que fan referencia a tratamentos de datos de carácter persoal que afecten ao funcionariado público ou calquera outro empregado contratado no seo da organización.

Directamente, isto levou consigo a revisión directa e actualización dos contratos subscritos cos encargados do tratamento, suxeitos que levan a cabo os tratamentos por conta do responsable e que deberán cumprir igualmente coas disposicións europeas e nacionais en materia de protección de datos.

A pesar de que é recomendable efectuar unha revisión dos contratos de acceso a datos, a LOPDGDD, por medio da súa disposición transitoria quinta, estableceu que os contratos perfeccionados con anterioridade ao 25 de maio de 2018, é dicir, antes da aplicación do RXPD, manterán a súa vixencia ata a data do seu vencemento e, en caso de que teñan carácter indefinido, a súa actualización poderase prorrogar ata o 25 de maio de 2022.

Así mesmo, as administracións públicas terán a obriga de asegurarse de que os encargados do tratamento seleccionados ofrecen garantías suficientes para aplicar medidas de índole técnica e organizativa apropiadas e, en consecuencia, que estas aseguren a protección dos datos persoais tratados conforme os preceptos recollidos na normativa, garantindo así a tutela dos dereitos dos afectados.

Nesta liña, cobran vital interese as directrices establecidas por parte das administracións públicas a través dos contratos de acceso a datos perfeccionados, xa que mediante a configuración destes derivarán as pertinentes responsabilidades xeradas como resultado dun incumprimento contractual ou, se é o caso, dun fallo de seguridade. Polo tanto, debe facerse especial fincapé nas estipulacións que fan referencia á facultade do encargado do tratamento para destinar os datos a finalidades diferentes para as cales se facilitaron, a posibilidade de comunicar eses datos a terceiros, é dicir, levar a cabo cesións de datos, así como acudir a terceiros para a prestación de determinados servizos e o xeito de proceder en caso de que teña lugar tal situación, séndolle de aplicación a este último encargado as mesmas obrigas que as que lle foron impostas ao encargado inicial. Tales obrigas serán exixidas a través dun contrato ou outro acto xurídico establecido conforme o dereito da Unión ou dos Estados membros.

De igual modo, terán que seguirse as instrucións dadas pola Administración pública, como responsable do tratamento, para poder levar a cabo as transferencias internacionais de datos de carácter persoal (en diante, TID), situación que se produce

cando estes se remiten fóra do ámbito do Espazo Económico Europeo[8]. Para tal efecto, non soamente deberá prestarse atención nas TID que teñan a súa orixe na propia actividade da Administración, senón que será especialmente relevante controlar e regular todas aquelas TID que se orixinan como corolario da evolución das tecnoloxías da información e comunicación, así como do uso, cada vez máis recorrente, dos servizos en nube (*cloud computing*)[9]. Neste extremo, cabe destacar que o texto europeo acrecenta os instrumentos a través dos cales se poderán realizar estas transferencias, entre os que se incorporan os xuridicamente requiridos e vinculantes entre autoridades e organismos públicos[10].

Pola súa vez, será fundamental establecer nos devanditos contratos o xeito de proceder do encargado do tratamento cando se produza unha fenda ou violación de seguridade dos datos persoais, é dicir, cando se "*ocasione a destrución, perda ou alteración accidental ou ilícita de datos persoais transmitidos, conservados ou tratados doutra forma, ou a comunicación ou acceso non autorizados aos ditos datos*"[11].

Nestes supostos, será indispensable establecer o prazo para a comunicación desas fendas de seguridade, o cal poderá ser superior a 24 horas, sendo recomendable que, á hora de perfeccionar o dito prazo no contrato, este preferiblemente non supere as 48 horas, posto que será o responsable do tratamento quen terá que notificarlle á autoridade de control competente tal acontecemento, sen dilación indebida e, como moito, dentro das 72 horas seguintes[12] desde que se producise a fenda de seguridade, sempre e cando esta constitúa un risco para os dereitos e liberdades dos afectados.

Isto implicará que, para a minimización dos riscos que se queiran asumir por medio do contrato, o encargado do tratamento facilite a información que a continuación se detalla, co fin de realizar unha axeitada e eficaz xestión, así como comunicación dos quebrantamentos acaecidos. Esa información deberá conter os seguintes puntos[13]:

a) Descrición da natureza da violación da seguridade dos datos persoais, mesmo, cando sexa posible, as categorías e o número aproximado de interesados afectados, e as categorías e o número aproximado de rexistros de datos persoais afectados.

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

9 Rfc. IBM Cloud. O *cloud computing* consiste na subministración, baixo demanda, de recursos informáticos a través de Internet e baseada nun modelo de pagamento por uso.

10 *Vid.* art. 46 do RXPD.

11 *Vid.* art. 4 do RXPD.

12 O considerando 85 do RXPD establece que, "*Se non se toman a tempo medidas axeitadas, as violacións da seguridade dos datos persoais poden entrañar danos e perdas* físicos, materiais ou inmateriais para as persoas físicas, como perda de control sobre os seus datos persoais ou restrición dos seus dereitos, discriminación, usurpación de identidade, perdas financeiras, reversión non autorizada da *pseudonimización, dano para a reputación, perda de confidencialidade de datos suxeitos ao segredo profesional, ou calquera outro prexuízo económico ou social significativo para a persoa física en cuestión. Por conseguinte, tan axiña como o responsable do tratamento teña coñecemento de que se produciu unha violación da seguridade dos datos persoais, o responsable debe, sen dilación indebida e, de ser posible, como moito 72 horas despois de que tivese constancia dela, notificar a violación da seguridade dos datos persoais á autoridade de control competente, a menos que o responsable poida demostrar, atendendo ao principio de responsabilidade proactiva, a improbabilidade de que a violación da seguridade dos datos persoais entrañe un risco para os dereitos e as liberdades das persoas físicas. Se a dita notificación non é posible no prazo de 72 horas, debe anexarse unha indicación dos motivos da dilación, podendo facilitarse información por fases sen máis dilación indebida*".

13 *Vid.* art. 33 do RXPD.

b) O nome e os datos de contacto do delegado de protección de datos ou doutro punto de contacto en que poida obterse máis información.

c) Descrición das posibles consecuencias da violación da seguridade dos datos persoais.

d) Descrición das medidas adoptadas ou propostas para pórlle remedio á violación da seguridade dos datos persoais, incluíndo, se procede, as medidas adoptadas para mitigar os posibles efectos negativos.

Por outro lado, nin a normativa internacional nin nacional ofrecen unha lista exhaustiva de todas as medidas de seguridade de carácter técnico e organizativo que deberán ser aplicadas en relación cos tratamentos efectuados. Neste sentido, e tal como se veu realizando ata o momento, as administracións públicas deberán aplicar todas as medidas contidas no Esquema Nacional de Seguridade (en diante, ENS), o cal establece aquelas ás cales convén adherirse en relación cos tratamentos de datos de carácter persoal efectuados.

Neste punto, a disposición adicional primeira da LOPDGDG incorpora o deber que teñen os responsables do tratamento para exixirlles aos encargados configurados como empresas ou fundacións suxeitas a dereito privado a adopción, no seo da súa organización, de medidas equivalentes ás establecidas polo ENS. Pola **súa vez,** este requisito será o aplicado naqueles supostos en que un terceiro preste un servizo en réxime de concesión, encomenda de xestión ou contrato, debendo corresponderse as medidas aplicadas coas da Administración pública de orixe.

Con todo iso pret**é**ndese alcanzar o cumprimento da protección de datos desde o deseño e por defecto[14], dous novos principios introducidos polo RXPD co propósito de que todas as organizacións e institucións respecten e avalen a privacidade da información dos titulares e, en consecuencia, cumpran con outro dos novos principios recollidos no texto europeo, a responsabilidade proactiva –tamén coñecido como *accountability*–.

En consecuencia, o responsable deberá documentar por medio dun rexistro de actividades do tratamento aquelas efectuadas baixo a súa responsabilidade, que veu substituír a obriga de notificarlles os ficheiros e tratamentos ás autoridades de control de protección de datos[15]. Pola súa banda, o encargado do tratamento terá a obriga de documentar no dito rexistro as categorías de actividades efectuadas por conta do responsable. Así as cousas, o rexistro de actividades do tratamento terá que manterse actualizado, xa que se trata dun documento vivo, debendo atoparse, en todo momento, á disposición das autoridades de control[16].

Unha vez documentadas esas actividades, será necesario realizar unha análise dos riscos que estas comportan –englobando tanto as xa existentes como as que

[14] Rfc. a AEPD na súa Guía "*Protección de Datos y Administración Local*" recolle que o principio de protección de datos desde o deseño supón que a protección de datos ha de estar presente nas primeiras fases de concepción dun proxecto e formar parte da lista de elementos a considerar antes de iniciar as sucesivas etapas de desenvolvemento. Así mesmo, entende que a protección de datos por defecto estriba en que só sexan obxecto de tratamento os datos persoais que sexan estritamente necesarios para cada un dos fins de tratamento.

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

vaian ter lugar–, para determinar se é pertinente realizar ou non unha avaliación de impacto sobre a protección de datos (en diante, AIPD). Neste sentido, as administracións públicas españolas contan actualmente con metodoloxías de análise e xestión de riscos, principalmente no ámbito dos sistemas da información, como, por exemplo, a norma *ISO 27005*, que derrogou as normas *ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000*, ou *MAGERIT*[17]. Esta última constitúese como unha metodoloxía de carácter público e atópase recoñecida por ENISA[18], configurándose como un instrumento que pretende posibilitar a implantación e aplicación do ENS[19].

Así mesmo, as AIPD deben ser realizadas con anterioridade á posta en marcha dos tratamentos e, cando se considere que estes entrañan unha serie de perigos para as liberdades e dereitos dos titulares, fixando pola súa vez unha secuencia de supostos en que será preceptivo realizar a dita avaliación. Non obstante, é certo que o texto europeo exceptúa a necesidade de realizar unha AIPD en tratamentos que non supoñen un alto risco para os dereitos e liberdades dos titulares, sempre e cando estes descansen sobre a base lexitimadora relativa á consecución de fins de interese público ou se atopen ligados ao fundamento referente ao exercicio dos poderes públicos. Tal como indicou a autoridade de control española, non se terán que someter a AIPD estes tratamentos, nos supostos de que exista unha norma que os regularice e se tivese realizado unha avaliación, como parte dunha AIPD xeral, no contexto da adopción desa norma de base[20].

Non é cuestión banal a importancia que radica en canto á cooperación que debe existir entre os responsables e encargados do tratamento, xa non só respecto ás continxencias acaecidas no marco da prestación de servizos, senón tamén en canto á correcta atención dos dereitos de acceso, rectificación, oposición, supresión, limitación e portabilidade dos datos exercitados polos titulares dos datos de carácter persoal. Para o exercicio deles, as administracións públicas deberán habilitar mecanismos sinxelos, accesibles e visibles para os cidadáns, así como establecer procedementos que impliquen a verificación da identidade do titular no suposto de que se permita o

17 Rfc. PORTAL ADMINISTRACIÓN ELECTRÓNICA, GOBERNO DE ESPAÑA. MAGERIT persegue estes obxectivos: i) concienciar os responsables das organizacións de información da existencia de riscos e da necesidade de xestionalos, ii) ofrecer un método sistemático para analizar os riscos derivados do uso de tecnoloxías da información e comunicación (TIC), iii) axudar a descubrir e planificar o tratamento oportuno para manter os riscos baixo control indirectos, iv) preparar a organización para procesos de avaliación, auditoría, certificación ou acreditación, segundo corresponda en cada caso.

18 A European Network and Information Security Agency (ENISA) é a Axencia da Unión Europea para a Seguridade das Redes e a Información, constituíndose como un centro de experiencia para a ciberseguridade, co que se pretende dotar a UE e os países que a conforman de consellos prácticos e solucións tanto ao sector público como privado, para previr, detectar e responder aos problemas que se orixinen como consecuencia da seguridade da información.

19 CN-CERT. CENTRO CRIPTOLÓXICO NACIONAL. A Lei 11/2007, do 22 de xuño, de acceso electrónico dos cidadáns aos servizos públicos estableceu o Esquema Nacional de Seguridade, que, aprobado mediante o Real decreto 3/2010, do 8 de xaneiro, ten por obxecto determinar a política de seguridade na utilización de medios electrónicos no seu ámbito de aplicación, e estará constituído polos principios básicos e requisitos mínimos que permitan unha protección axeitada da información. Posteriormente, a Lei 40/2015, do 1 de outubro, de réxime xurídico do sector público, recolle o Esquema Nacional de Seguridade no seu artigo 156, apartado 2, en similares termos. En 2015 publicouse a modificación do Esquema Nacional de Seguridade a través do Real decreto 951/2015, do 23 de outubro, en resposta á evolución do ámbito regulatorio, en especial da Unión Europea, das tecnoloxías da información e da experiencia da implantación do esquema.

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

exercicio de tales dereitos a través de medios electrónicos, como por exemplo remitir unha copia do documento nacional de identidade.

Retomando a importancia do deber de colaboración descrito, será determinante establecer o prazo que ten o encargado do tratamento para darlle traslado ao responsable das solicitudes formuladas polos afectados polos tratamentos dos seus datos de carácter persoal, así como establecer a imposición de medidas axeitadas co fin de garantir a correcta recepción destas, no caso de que non se lle atribúa a facultade de contestación a tales peticións ao encargado do tratamento. Igualmente, estas cuestións deberán ser reflectidas no contrato subscrito entre ambas as dúas partes.

En canto á figura do delegado de protección de datos, este revístese de carácter obrigatorio, cabendo a posibilidade de nomear un único delegado para varios organismos, aínda que é certo que tal decisión terá que atender ao tamaño e á estrutura da dita entidade pública. Así mesmo, os delegados, tal como indica o considerando 97 do RXPD, deberán posuír coñecementos especializados en dereito e a práctica en materia de protección de datos. Finalmente, terán que ser establecidas as unidades nas cales este será integrado e a posición que ten dentro do ente público, debendo ser habilitados mecanismos que permitan aos cidadáns contactar con el, como por exemplo a través da inclusión, dentro da política de privacidade da páxina web ou nos formularios que se atopen á disposición do público, do seu correo electrónico.

Por último, todas as directrices que se foron mencionando ao longo deste estudo e que supoñen, en definitiva, unha exposición dos puntos máis relevantes que afectan dun xeito directo á Administración pública e aos seus provedores de servizos deberán atoparse suxeitas ao deber de segredo e confidencialidade.

Bibliografía

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

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

CARRIÓN GARCÍA DE PARADA, F.J., e 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 (xaneiro-abril) 2018.

JIMÉNEZ ASENSIO, R., e MORO, A., *Manual-guía sobre impactos del Reglamento (UE) de protección de datos en los entes locales*, Federació de Municipis de Catalunya, 2018. Dispoñible 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. Dispoñible 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*, maio 2018.