MARIANO MAGIDE

Abogado. Uría Menéndez

URÍA MENÉNDEZ

La nueva Ley de Contratos del Sector Público: novedades y retos

Las sociedades de economía mixta, podrán seguir siendo utilizadas como instrumentos de gestión indirecta de servicios públicos

La nueva Ley apuesta también por una mayor transparencia en la contratación y por un mayor control

La nueva Ley de Contratos del Sector Público responde en lo fundamental a la necesidad de transponer las Directivas de contratos y concesiones de 2014. Siendo así, no resulta fácil encontrar directrices generales que den un sentido unitario a la reforma. A falta de ese hilo conductor, se harán a continuación algunas reflexiones sobre los aspectos más relevantes de la nueva Ley, con una específica referencia final a la regulación de las concesiones de obras y servicios.

Intentando buscar orientaciones de política legislativa en la reforma, cabe referirse en primer lugar a su apuesta por la incorporación de criterios sociales en la contratación pública y por una mayor apertura de esa contratación a las pymes. Esta orientación encuentra su límite, lógicamente, en la necesidad de que los procedimientos de contratación estén dirigidos a la adjudicación de los contratos a las mejores ofertas, lo que habrá siempre de hacerse de acuerdo con los principios de transparencia, igualdad y no discriminación entre los empresarios que liciten.

La nueva Ley apuesta también por una mayor transparencia en la contratación y por un mayor control. Se intensifican así, por ejemplo, las obligaciones de información de los sujetos del sector público a través de sus perfiles de contratante. Desde la perspectiva del control, se establece una regulación más estricta de la utilización por parte de la Administración de medios propios personificados y se realiza una regulación de las modificaciones de los contratos que, si bien elimina alguna de las excesivas rigideces introducidas por la Ley de Economía Sostenible de 2011, incluye mayores limitaciones que las necesariamente impuestas por las Directivas. En un intento de que el empleo de medios propios y las modificaciones de contratos preexistentes no hurten al mercado nuevas licitaciones, se extiende el recurso especial en materia de contratación a este tipo de decisiones.

Incremento del control sobre la contratación pública

La Ley incorpora también novedades procedimentales y organizativas inspiradas en esta voluntad de incrementar el control sobre la contratación pública. Entre las primeras se puede contar la sustitución de los procedimientos negociados sin publicidad por el procedimiento abierto simplificado. Entre los segundos, la creación de la Oficina Independiente de Regulación y Supervisión de la Contratación, bien intencionada, aunque quizá no suficientemente decidida, a la vista de la escasa estructura de la que se dota a esta Oficina.

La Ley transpone también la Directiva de concesiones, cuyo concepto gira alrededor de la asunción por el concesionario del «riesgo operacional» en la explotación de la obra o el servicio. Esa transposición se lleva a cabo de un modo excesivamente literalista, dando así lugar a novedades que no vienen impuestas realmente por la Directiva de concesiones y que no resultan de fácil justificación objetiva.

En efecto, la Ley, al socaire de la transposición de la Directiva, reduce a dos los diferentes contratos típicos que han venido permitiendo la colaboración entre el sector público y los empresarios para la provisión de obras y servicios públicos: la concesión de obras y la de servicios (sea o no de servicios públicos en sentido propio).

Desaparición del contrato de colaboración

Desaparecen como contratos típicos el poco empleado contrato de colaboración entre el sector público y el sector privado, y los subtipos del actual contrato de gestión de servicios públicos distintos del de concesión. No obstante, la Ley mantiene una expresa referencia a las sociedades de economía mixta, que podrán seguir siendo utilizadas como instrumentos de gestión indirecta de servicios públicos, mediante la atribución directa a ese vehículo institucional de cooperación de una concesión de servicios, siempre que el privado haya entrado en ella mediante un procedimiento de adjudicación de los que la Ley prevé para la adjudicación de las concesiones.

Por lo que al tan traído y llevado «riesgo operacional» respecta, en mi opinión no estamos ante un concepto sustancialmente distinto del tradicional riesgo y ventura en la explotación de las concesiones. No exige, pues, la Directiva, una mayor traslación de riesgos a los privados, a la que parece apuntar la nueva regulación de las causas de mantenimiento del equilibrio económico del contrato y de los efectos económicos de la resolución de las concesiones, excesivamente tributaria del famoso asunto de las «radiales». Una distribución de riesgos inadecuada entre el sector público y el privado puede perjudicar la inversión privada en infraestructuras, de la que España está necesitada y por la que compite con el resto de las jurisdicciones.

En esto, como en otros aspectos de la nueva Ley, la práctica contractual, a través de un adecuado diseño de los pliegos, será fundamental para aprovechar al máximo las potencialidades de la nueva norma y minimizar sus defectos. Ese será el principal reto tras su entrada en vigor el próximo 9 de marzo.

SONIA VÁZQUEZ

Abogada de Ecija

ECIJA

Las brechas de seguridad en el RGPD

Ninguna entidad, sea pública o privada, queda a salvo de ser objeto de un ciberataque

Las empresas deberán proceder a implantar los protocolos de notificación de brechas de seguridad pertinentes

El nuevo Reglamento General de Protección de Datos (en adelante, RGPD) viene a introducir una serie de novedades a tener en cuenta en aquellos casos en los que cualquier empresa sufra una brecha de seguridad. En esta línea, el grupo de trabajo del artículo 29, ha venido a desarrollar una *guideline* que señala las directrices sobre notificación de las violaciones de seguridad de los datos personales, de acuerdo con el Reglamento 679/2016.

Lo novedoso se encuentra en que antes de la entrada en vigor del RGPD, la obligación de notificar las brechas de seguridad o violaciones de seguridad, se limitaba a los operadores de servicios de comunicaciones electrónicas disponibles al público, tal y como se señalaba en la Ley 9/2014 General de Telecomunicaciones y en el Reglamento (UE) nº 611/2013 de la Comisión (recogido en la Directiva 2002/58/EC, más conocida como Directiva E-Privacy).

El propio RGPD señala que se entenderá que existe una brecha de seguridad o una violación de seguridad de los datos en aquellos casos en los que la «*violación de la seguridad 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*».

A título ejemplificativo, podemos señalar algunos de los incidentes de seguridad más importantes acontecidos en los últimos años, como el caso de *Yahoo*!, que fue víctima de una de las brechas de seguridad más grandes de la historia, al ser objeto de robo de los datos personales de millones de usuarios (incluyendo nombres, direcciones de correo electrónico, números de teléfono, fechas de nacimiento y contraseñas). También el Departamento de Justicia de EE.UU. fue objeto de ataque, y nombres, cargos, números de teléfono y direcciones de correo electrónico fueron robados y filtrados. Recientemente, Uber confirmó que había sufrido una brecha de seguridad en octubre de 2016 y que información de carácter personal de millones de usuarios de su aplicación había sido expuesta. Como agravante, la compañía optó por ocultar esta brecha de seguridad, cediendo a la extorsión de los ciberdelincuentes con el fin de que borrasen los datos personales robados y la filtración de estos no trascendiese.

Ninguna entidad, sea pública o privada, queda a salvo de sufrir una brecha de seguridad o de ser objeto de un ciberataque, por lo que este punto pasa a convertirse en primordial para todas ellas, no sólo desde el punto de vista de cumplimiento normativo, sino también desde aquel que afianza a la entidad en el mercado y garantiza a los terceros la fiabilidad y seguridad de las medidas de seguridad implementadas en la misma.

Obligación de notificar a la autoridad

Una de las principales novedades que el RGPD impone a los responsables de tratamiento de datos de carácter personal, es la obligación de notificar a la autoridad de control de aquellas brechas de seguridad que constituyan un riesgo para los derechos y las libertades de las personas físicas. En este sentido, deberán tenerse en cuenta diferentes criterios a la hora de determinar si se ha producido tal riesgo, como son: el tipo de brecha sufrida; la naturaleza, volumen y carácter sensible de los datos personales afectados; la gravedad de las posibles consecuencias para los titulares de los datos (daños morales, económicos, reputacionales, etc), que la violación de seguridad afecte a categorías especiales de datos e incluso las características específicas del responsable del tratamiento.

En aquellos casos en los que la empresa determine que la brecha de seguridad constituya un riesgo para los derechos y libertades de las personas físicas, deberá, en todo caso, proceder a su notificación a la autoridad de control sin dilación indebida y, a más tardar, 72 horas después de que haya tenido constancia de ella. Si dicha notificación no es posible en el plazo de 72 horas, deberá acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida. Como mínimo, esta notificación deberá contener una descripción de la naturaleza de la violación de seguridad (incluyendo, cuando sea posible, las categorías y número aproximado de afectados y de registros de datos personales afectados), así como los detalles de contacto del DPO de la empresa, las posibles consecuencias de la brecha de seguridad y las medidas de seguridad adoptadas o propuestas por el responsable del tratamiento.

Además, en aquellos casos en los que la brecha de seguridad entrañe alto riesgo para los derechos y libertades de las personas físicas, el RGPD establece la obligación de notificar a los interesados de la misma, sin dilación indebida. Sin embargo, matiza que en aquellas ocasiones en las que el responsable haya adoptado medidas técnicas u organizativas apropiadas antes de que se produjese la brecha de seguridad, tomado medidas posteriores que mitiguen y resuelvan dicha violación o cuando dicha comunicación suponga un esfuerzo desproporcionado, no será necesario realizar esta comunicación.

Los encargados del tratamiento

Es importante señalar que la notificación de brechas de seguridad atañe también a los encargados del tratamiento que en su caso existiesen, quedando estos obligados a notificar cualquier brecha de seguridad de la que tengan conocimiento a los responsables del tratamiento, de nuevo sin dilación indebida.

Entre otras de las obligaciones que prevé el RGPD, el responsable del tratamiento deberá disponer de un registro de brechas de seguridad, en el cual deberá dejar reflejado todo incidente que tenga lugar, incluyendo los hechos relacionados con este, sus efectos y las medidas correctivas adoptadas, de tal forma que las autoridades de control puedan en todo momento verificar el cumplimiento del responsable respecto a sus obligaciones.

Como ya apuntábamos, además de que el incumplimiento de los requerimientos expuestos en el RGPD puede acarrear a la organización una multa administrativa superior a los 10 millones de euros o de una cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, no debemos de perder de vista que estos incidentes de seguridad suelen conllevar nefastas consecuencias en lo que efectos reputacionales se refiere, lo cual en muchos casos resulta a las empresas incluso más gravoso que la propia sanción económica.

En base a lo expuesto, las empresas deberán proceder a implantar los protocolos de notificación de brechas de seguridad pertinentes, con el fin de dar cumplimiento a las nuevas obligaciones establecidas en el RGPD, y en todo caso, adoptar las correspondientes medidas de seguridad con el fin de evitar, en lo posible, ser objeto de ciberataques y filtraciones de datos personales que acarreen gravosas consecuencias.