Breves consideraciones sobre la ciberseguridad y su implementación en la Contratación Pública.

Jorge Fondevila Antolín

1. Consideraciones Previas.

Este breve comentario es un resumen del artículo publicado en la Revista de Contratación Administrativa Práctica (LA LEY/Wolters Kluwer)[1] donde se examina de forma amplia y detallada el marco normativo establecido por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante (ENS) y su aplicación a la Contratación Pública, disponible en este enlace: https://bit.ly/423MC1q

Como ya he expuesto en trabajos anteriores[2], la seguridad de la información, en directa conexión con la protección de datos personales, constituye uno de los basamentos fundamentales en el desarrollo de la contratación pública electrónica, pues solo desde la confianza y seguridad pueden desarrollarse adecuadamente los procedimientos de licitación y la implementación de la e-contratación y su necesaria y permanente innovación[3].

Así, podemos formular unas consideraciones previas esenciales:

a) No hay administración digital con seguridad jurídica, sin una adecuada seguridad de la información y de los datos personales en poder de la administración

[1] FONDEVILA ANTOLIN, J. "Régimen jurídico de la ciberseguridad en la contratación pública: un gran olvidado, pero con importantes consecuencias por su incumplimiento", *Revista Contratación Administrativa Práctica*, LA LEY/Wolters Kluwer, Madrid, Septiembre, (2023) en prensa.

[2] FONDEVILA ANTOLIN, J., "Seguridad en la utilización de medios electrónicos. El Esquema Nacional de Seguridad", en Director: Eduardo Gamero Casado; Coordinadores: Severiano Fernández Ramos y Julián Valero Torrijos: *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del Sector Público*, Tirant lo Blanch, Valencia, (2017), págs. 598 y ss. y "La Seguridad de la información y la Protección de datos en las plataformas de contratación electrónica "Cloud computing": Descripción de las características técnicas y su régimen jurídico", en Dir. Jaime Pintos Santiago, "*Las consecuencias electrónicas de la nueva ley de contratos del sector público: Código electrónico práctico de la nueva Ley 9/2017 de Contratos del Sector Público*", Punto Rojo Libros, S.L., Sevilla, 2018/a, págs. 203 y ss. Asimismo, a este respecto también resulta recomendable la consulta de CANALS AMETLLER, D. (Dir.), en "Ciberseguridad: un nuevo reto para el Estado y los Gobiernos Locales", El Consultor – Wolters Kluwer, Madrid, 2021.

[3], Con relación al régimen jurídico general del uso de los medios electrónicos en la contratación estimamos adecuado para un examen general destacar algunas obras MARTÍNEZ GUTIÉRREZ, R. "*La Contratación pública electrónica*", Aranzadi, Cizur menor, 2015, también SÁNCHEZ GARCÍA. A. "*La transformación electrónica de la contratación pública. De la digitalización a la automatización*", Tecnos, Madrid, 2022, y asimismo, DOMINGUEZ-MACAYA LAURNAGA, J. "*La contratación pública electrónica*", El Consultor - Wolters Kluwer, Madrid, 2022; finalmente con relación a la innovación es de destacar el trabajo de "VAZQUEZ MATILLA, F.J., "Retos de la transformación digital en la contratación pública", *Revista Contratación Administrativa Práctica* nº 182, 2022.

b) No es posible implementar una licitación electrónica que resulte respetuosa con las obligatorias garantías procedimentales, especialmente, las referidas al secreto de las ofertas, si no podemos garantizar que nuestros sistemas de información cumplen las exigencias técnicas legalmente establecidas.

c) Dicho lo anterior, es necesario realizar una consideración general, en concreto, la seguridad de la información debe ser examinada desde una doble perspectiva, una (*ad intra*) y que se desarrolla en torno a la puesta en funcionamiento de los medios electrónicos necesarios para la implementación de la licitación, es decir, nos referimos a las necesarias plataformas de gestión administrativa para las fases preparatoria y de ejecución de los contratos y otro tipo de plataformas específicas para la licitación electrónica[4], y por otro lado, existe otro ámbito, de gran importancia pero que suele pasar desapercibido, (*ad extram*), referido a las exigencias y relaciones a establecer con los licitadores y adjudicatarios de los contratos en materia de seguridad de la información y por ende, de la protección de datos[5].

d) El nuevo marco normativo del R.D. 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, en adelante (ENS), impone la adopción de medidas técnicas de ciberseguridad que afectan no solo al uso de instrumentos digitales en el desarrollo y gestión administrativa de la licitación, sino que su ámbito se ha ampliado al cumplimiento de requisitos y certificaciones de los sistemas de información y soluciones informáticas objeto de las licitaciones.

e) Es importante tener en cuenta que la obligación de cumplimiento de las obligaciones establecidas en el ENS, no son nuevas pues se encuentran en vigor desde el año 2010, en que se aprobó el Real Decreto 3/2010, de 8 de enero, y, por lo tanto, nos encontramos no ante una nueva situación fáctica y normativa, sino simplemente ante una revisión y actualización del citado marco técnico, como confirman las previsiones de la Disposición Transitoria única del R.D. 311/2022.

Es decir, a nuestro juicio, la norma está confirmando que los sistemas de información y soluciones informáticas que utilizan las administraciones públicas en la gestión de los procedimientos de licitación ya deberían estar certificados hace años conforme al ENS, especialmente las plataformas de licitación que se están utilizando por parte de nuestras administraciones públicas[6]. A este respecto,

---

[4]A este respecto, resulta recomendable la consulta de ALAMILLO DOMINGO, I., "Innovación y seguridad en la contratación pública. Especial referencia a la presentación y recepción electrónica de ofertas", en Coordinación: Concepción Campos Acuña, La Nueva contratación pública en el ámbito local, El Consultor - Wolters Kluwer, Madrid, 2017; también nos remitimos a nuestros trabajos FONDEVILA ANTOLIN, J., opus. cit. 2018/a y finalmente "La Subasta electrónica", en Dir. Gamero Casado y Gallego Córcoles *Tratado de Contratos del Sector Público*, Tirant lo Blanch, Valencia, 2018/b, págs. 2020 y ss.

[5] Destacamos a este respecto el trabajo de SERNA BARDAVIO, D., "La Protección de datos en la contratación pública, ¿expectativa o realidad?, *Revista Contratación Administrativa Práctica* nº 182, (2022).

[6] A este respecto, es importante comprobar como todavía la mayoría de Administraciones sigue incumpliendo esta obligación, así se puede comprobar consultando la web del ccn.cni: https://gobernanza.ccn-cert.cni.es/certificados

ya nos hemos manifestado en múltiples ocasiones[7] sobre este grave incumplimiento en alguna plataforma de gran utilización, que además no reúne la condición de sede electrónica, de manera que las notificaciones que se practiquen a través de la misma[8], resultan nulas de pleno derecho al infringir las previsiones del artículo 43 de la Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC), es un gran riesgo que puede generar en determinas condiciones graves responsabilidades para las administraciones públicas que utilicen estas plataformas sin certificación del ENS, como explicaremos al final de este trabajo.

Asimismo, esta disposición en estos mismos términos también resulta de aplicación a los sistemas de información y soluciones de titularidad de entidades privadas, a este respecto resulta de gran interés la Resolución nº 1132/2022 del Tribunal Administrativo Central de Recursos Contractuales (TACRC) de 29 de septiembre de 2022.

2. El Ámbito de aplicación subjetivo y material del ENS con relación a la Contratación Pública.

Es importante destacar los cambios que ha incorporado las nuevas previsiones del artículo 2.1 del (ENS), De una simple lectura del precepto podemos observar que se ha ampliado de forma sustancial su ámbito de aplicación, ya que, incorpora a las "*Las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas*", y también a "*Las Universidades públicas*". Así pues, con relación a las Administraciones Públicas en su sentido clásico continúan bajo el mandato de cumplimiento del ENS, la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades Locales y cualesquiera organismos públicos y las entidades de derecho público vinculados o dependientes de estas Administraciones Públicas.

Dicho esto, es preciso también constatar otra esencial novedad del ENS a este respecto, nos referimos a la exigencia en el artículo 2.3 de cumplimiento por los sistemas de información de las entidades del sector privado de las exigencias del ENS, pero siempre que concurran determinadas circunstancias, y que serán objeto de examen de detalle en los apartados posteriores.

En cuanto al ámbito material, destacan las nuevas previsiones sobre exigencia de cumplimiento del ENS para las entidades del sector privado, en su condición de proveedores de las Administraciones Públicas y sus límites. Así, resulta destacable la nueva regulación de los artículos 2.3 y 12 del ENS, estas previsiones están suscitando mucho debate entre los gestores y especialmente

[7] Por todas nos remitimos a FONDEVILA ANTOLIN, J., op, cit. 2018/a, págs. 203 y ss.
[8] Sobre las notificaciones resulta de gran interés los trabajos de MARTIN DELGADO, I. "La Difusión e intercambio de información contractual a través de medios electrónicos. Publicidad, notificaciones y comunicaciones electrónicas", en Dir. Gamero Casado y Gallego Córcoles, *Tratado de Contratos del Sector Público*, Tirant, Valencia, 2018, págs. 1951 y ss. También, MORENO MOLINA, J.A. "Comunicaciones, notificaciones, identificación y firma en la contratación pública", en Dir. Martin Delgado y Moreno Molina, "*Administración electrónica, transparencia y contratación pública a nivel autonómico*", Iustel, Madrid, 2021, págs. 193 y ss.

entre los servicios informáticos dado que puede afectar directamente a las licitaciones originadas en sus servicios, y ello, por cuanto, se ha producido alguna interpretación para la cual esta previsión supone una obligación general de cumplimiento del ENS (incluida una política de seguridad aprobada y en su caso, acreditada) por toda empresa que contrate servicios de información o soluciones de cualquier clase con las administraciones. Desde luego esta interpretación podría ser un hándicap muy grande para los licitadores, que podría dejar fuera a un gran número de ellos, lo que, a su vez podría suponer una colisión con la Directiva 2014/24/UE. Dicho lo anterior, podemos afirmar que esta interpretación no se corresponde, a nuestro juicio, por las razones que exponemos el artículo de consulta con la "ratio legis" del ENS, y también por las respuestas del CCN-CNI, incorporadas al Anexo del citado trabajo, a las consultas realizadas a ese centro. Asimismo, resulta imprescindible para una adecuada interpretación de las previsiones del ENS, proceder a una delimitación y alcance de los conceptos técnicos: servicios de información, soluciones informáticas y servicios de seguridad de la información, a este respecto nos remitimos a nuestro artículo.

3. La incorporación a los Pliegos de cláusulas administrativas de los requisitos subjetivos y materiales exigidos por el ENS.

Conforme lo expuesto anteriormente, entendemos que resulta necesario examinar la ubicación sistemática y legal de las exigencias legales establecidas en el ENS en los correspondientes Pliegos de cláusulas administrativas particulares y en los Pliegos de prescripciones técnicas, estas decisiones tienen gran transcendencia, por cuanto su calificación jurídica, condiciona los efectos a desplegar tanto en el proceso de licitación como en la ejecución del contrato, ya que las mismas pueden generar diferentes consecuencias en el caso de su no cumplimiento. Así, nuestra exposición examinara dos ámbitos claramente diferenciados por el ENS, la exigencia de que los servicios de información utilizados por las entidades privadas, incluido tener aprobada su política de seguridad, se encuentren certificados de conformidad con el ENS (requisito subjetivo), y, por otro lado, las exigencias específicas de certificación de las soluciones suministradas por estas entidades privadas (requisito material).

A) La exigencia de que los sistemas de información utilizados por las entidades privadas para prestar servicios se encuentren certificados de conformidad con el ENS.

Esta previsión supone, a nuestro juicio, que nos encontramos en el ámbito normativo establecido por el artículo 65.2 de la Ley 9/2017, de 8 de noviembre (LCSP), que establece: "Los contratistas deberán contar, asimismo, con la habilitación empresarial o profesional que, en su caso, sea exigible para la realización de las prestaciones que constituyan el objeto del contrato". A esta consideración debemos añadir algunos pronunciamientos del Tribunal Administrativo Central de Recursos contractuales que resultan sumamente ilustrativos, así, Resolución nº116/2015 de 6 de

febrero de 2015, Resolución nº 214/2021 de 5 de marzo de 2021, Resolución 1099/2021 de 9 de septiembre de 2021 y la Resolución nº 532/2022 de 13 de mayo de 2022.

A nuestro juicio, entendemos que la acreditación de contar con la correspondiente certificación de cumplimiento del ENS por las entidades privadas que pretendan licitar, cuando estemos en presencia de contratos de prestación de servicios de información para el ejercicio por las entidades públicas de sus competencias y potestades administrativas, especialmente (in cloud), se configura como un requisito de "habilitación profesional", de manera que su no acreditación conllevará necesariamente su exclusión de la licitación. Cuestión diferente es la aplicación de esta exigencia a las licitaciones de "soluciones informáticas" a medida o las específicas de ciberseguridad, pues con relación a las primeras no resultaría exigible, dado que en ese caso la exigencia se predica sobre la solución y no sobre el servicio de información, y esta diferencia es clave, pues las entidades privadas no intervienen, conexionan o resultan interoperables de forma permanente y directa en su implementación, y en cuanto a las segundas, además de resultar de aplicación las mismas razones, hay que tener en cuenta que estas cuentan con su específica regulación, y finalmente, con relación a las soluciones "Off the Shelf", tampoco resultaría exigible esta habilitación, y ello, en concordancia con las mismas razones expuestas con relación a las soluciones a medida.

B) Exigencia de que los servicios de información o soluciones ofertados por las entidades privadas se encuentren certificados de conformidad con el ENS.

En este apartado nos enfrentamos a otra cuestión esencial en la elaboración de los Pliegos de cláusulas administrativas particulares y Pliegos de Prescripciones técnicas, en concreto, la ubicación de la exigencia legal del ENS de incorporar a los Pliegos la exigencia de que los sistemas de información y soluciones prestados a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas acrediten el cumplimiento de las exigencias del ENS, las preguntas a las que nos enfrentamos serían las siguientes: ¿estamos ante un requisito de solvencia técnica?, o ¿ante una condición especial de ejecución?, o bien, ¿ante una condición técnica de obligado cumplimiento conforme el PPT?, la solución no es fácil, dado que nos encontramos ante un nuevo marco normativo que a diferencia de lo ocurrido con relación a la materia de Protección de Datos Personales, no ha sido integrada en la legislación contractual, a nuestro juicio, lo correcto hubiera sido una necesaria modificación de las previsiones de la LCSP, que hubiera aportado seguridad jurídica tanto a los gestores como a los operadores jurídicos.

En nuestro artículo, al que nos remitimos, desarrollamos con amplias consideraciones las razones que amparan las siguientes conclusiones:

1. La solvencia técnica y la acreditación de cumplimento del ENS de un sistema de información o solución, no es instrumento adecuado para cumplimentar las exigencias del ENS.

2. La acreditación de cumplimento del ENS de un sistema de información o solución, como “condición especial de ejecución”. En principio tampoco es el instrumento adecuado, salvo en el caso de las soluciones “ad hoc” o a medida, es decir, nos referimos a aplicaciones diseñadas específicamente y adaptadas a los concretos servicios de una administración, y ello, por cuanto, en estos casos existen un impedimento material esencial para reconducir a este tipo de soluciones al instrumento de las "condiciones técnicas", pues en términos ilustrativos, una aplicación informática que deberá diseñarse de forma específica y adaptada a los sistemas de una Administración Pública, es casi imposible que pueda obtener la previa y necesaria certificación de conformidad con el ENS, ya que el encargo es precisamente su elaboración e implementación específica, de manera que no es posible certificar algo que todavía no existe, y por ello, consideramos que solo en esta clase de supuestos, la exigencia de conformidad con el ENS, debe ser reconducida a una "condición especial de ejecución", cuyo cumplimento se acreditara durante la fase de ejecución del contrato, que es el momento en que existiría un producto a certificar.

3. La acreditación de cumplimento del ENS de un sistema de información o solución, como “condición técnica” incorporada a los Pliegos de prescripciones técnicas. Es la solución que estimamos más correcta para su incorporación al Pliego de Prescripciones Técnicas, y esta sería aplicable a los siguientes supuestos:

a) Los Sistemas de Información, en los términos técnicos fijados por el ENS, y explicados con mayor detalle en el artículo.

b) Las soluciones informáticas de ciberseguridad, en los términos exigidos en el artículo 19 y Anexo II del ENS.

4. Finalmente, tenemos un último grupo, las soluciones informáticas de mercado o "Off the Shelf", en este caso no podemos establecer una aplicación directa de las exigencias de certificación del ENS, pero eso no supone como destaca el CCN-CNI, que no se deba realizar por las Administraciones Públicas una evaluación individualizada de los riesgos de seguridad, antes de su adquisición. Efectivamente, el que no resulten exigibles desde un criterio jurídico formal las certificaciones del ENS, no significa que no deban exigirse e incorporarse las correspondientes medidas de seguridad por parte del Responsable de Servicio (órgano de contratación), conforme las funciones asignadas en el artículo 41 del ENS, en los Pliegos de prescripciones técnicas, bajo la calificación de "condiciones de ejecución".

4. Los Efectos derivados del incumplimiento de las previsiones del ENS en la contratación pública.

A) La Seguridad de la información y efectos sobre los Pliegos que incumplan las previsiones del ENS.

Las posibles consecuencias de una infracción de las previsiones de las exigencias del ENS en la implementación de los procesos de contratación, y para ello, comenzamos por el estudio de las causas de nulidad de los procedimientos de contratación[9]. Así, el marco normativo viene determinado por las previsiones del artículo 39 de la LCSP, que establece dos ámbitos materiales normativos de declaración de nulidad, a saber, los derivados de las previsiones del artículo 47 de la Ley 39/2015 LPAC, y en segundo lugar los específicos establecidos en el apartado segundo del citado artículo 39 de la LCSP.

B) Seguridad de la información y Responsabilidad Patrimonial de la Administración.

La responsabilidad no solo se genera por un funcionamiento anormal de la seguridad de la información, sino que especialmente aparecería esta, a nuestro juicio, en el caso de que la correspondiente administración no adoptara medidas de seguridad en sus sistemas de información y soluciones informáticas exigidas por el Esquema Nacional de Seguridad, atención a la certificación de conformidad con el ENS de las Plataformas de Licitación, así, la inacción en materia de seguridad entendemos que también originara de inmediato la posibilidad de responsabilidad de la administración en el caso de que se produzca algún incidente de seguridad que provoque o pueda provocar daños de cualquier clase por el acceso ilegal o pérdida de los datos de carácter personal de un ciudadano o empresa, sin olvidar que en este sentido incluimos también todos los datos de carácter económico de las empresas. Asimismo, tampoco resulta eximente una posible alegación de las previsiones del artículo 34 de la LRJSP cuando este condiciona el derecho a la indemnización a que el particular no tenga el deber jurídico de soportar el daño, como destaca Valero Torrijos[10], aunque con referencia supuestos daños generados por la aplicación de Inteligencia Artificial, pero que estimamos trasladable a esta situación, si la Administración Pública opta por utilizar medios electrónicos en sus relaciones con los ciudadanos esta debe dar cumplimiento a las exigencias legales del ENS, y si no lo hace, los ciudadanos no tienen deber alguno de soportar el daño generado. Además, tampoco es posible la alegación de

[9] Para un examen integral de esta materia nos remitimos al trabajo de DIEZ SASTRE, S. "La invalidez de los Contratos Públicos", en Dir. Gimeno Feliu Estudio sistemático de la Ley de Contratos del Sector Público, Aranzadi, Cizur menor, (2018), págs.571 y ss.

[10] VALERO TORRIJOS, J. "Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración", *Revista catalana de dret públic* nº 58, 2019.

existencia de un supuesto de "fuerza mayor", por cuanto, el incumplimiento de las exigencias legales descarta ad *radice* esa posibilidad.