Oficina Antifrau
de Catalunya

Sistemas automatizados de alerta en el ámbito de la contratación pública

Estudio

La Oficina Antifraude es una institución independiente, adscrita al Parlamento de Catalunya, encargada de prevenir e investigar la corrupción así como preservar la transparencia y la integridad de las administraciones y el personal al servicio del sector público en Catalunya.

En noviembre de 2020 la Dirección aprobó la *Memoria inicial de la estrategia de inteligencia basada en análisis de datos de la Oficina Antifraude de Catalunya*, con el objetivo de dotarse de una estrategia propia en el ámbito de la inteligencia basada en el análisis de datos (*data-driven intelligence*), al servicio de la misión y de las funciones de la Oficina. El horizonte temporal de esta iniciativa es de tres años, 2021 a 2023, y para su desarrollo se ha constituido un grupo de trabajo dedicado, el Equipo de Análisis de Datos.

Este estudio es el primer producto de aquella estrategia, correspondiente al primero de los proyectos que la integran, desarrollado a lo largo del año 2021. Su objetivo es determinar el estado de situación, estudiar los referentes existentes y formular algunas orientaciones y recomendaciones a fin de fomentar el diseño e implementación de sistemas automatizados de alerta en el ámbito de la contratación pública.

Oficina Antifrau de Catalunya | Equipo de Análisis de Datos
Autor: Bruno González Valdelièvre

Septiembre de 2022 (versión española)

www.antifrau.cat | bustiaoac@antifrau.cat

Oficina Antifrau de Catalunya

Equip d'Anàlisi de Dades

Sistemas automatizados de alerta en el ámbito de la contratación pública

Índice

0 Resumen ejecutivo

Este estudio trata de los **sistemas automatizados de alerta en el ámbito de la contratación pública**, definidos como sistemas tecnológicos que, procesando mediante los correspondientes algoritmos datos de diversas fuentes, tanto intrínsecas a los procedimientos de contratación como extrínsecas a los mismos, detecten y pongan automatizadamente en conocimiento de las instancias de control, internas y/o externas, la existencia o la posibilidad —y, eventualmente, en estos casos, la probabilidad—de irregularidades y, en su caso, impiden su efectiva materialización.

El interés y la oportunidad de este estudio se justifican por la coincidencia de una serie de tendencias estructurales y, al mismo tiempo, de una circunstancia coyuntural que, convergiendo en el momento actual, generan **una ventana de oportunidad** en esta vertiente de la lucha contra el fraude y la corrupción, que debería ser aprovechada por todas las instancias e instituciones con un compromiso firme con la integridad en la gestión pública.

Las **grandes tendencias de fondo** que favorecen el desarrollo de los sistemas de alerta de esta naturaleza son, en primer lugar, el desarrollo de un **marco legal** que impulsa y, en cierta medida, impone la tramitación electrónica de los procedimientos administrativos, especialmente de los procedimientos de contratación; este marco legal ya ha alcanzado una cierta madurez especialmente en Catalunya, con la promulgación del Decreto 76/2021, de 4 de agosto, de Administración digital.

En segundo lugar, también tienen una indudable relevancia la **consolidación de los paradigmas de la transparencia y los datos abiertos**, que se han ido implantando, normativa y operativamente, en la última década.

Estas tendencias han dado lugar al desarrollo y a la progresiva implementación en los diversos niveles del sector público —local, autonómico y estatal— de soluciones tecnológicas para la tramitación íntegramente electrónica de los procedimientos, dando lugar al fenómeno de la ***datificación* de la actividad del sector público**. Es decir, la generación por la propia tramitación administrativa de datos en soportes electrónicos susceptibles de ser recopilados, almacenados, tratados y explotados con múltiples finalidades y, entre ellas, y a los efectos que aquí nos interesan, al servicio de la integridad, para la prevención, detección, corrección y persecución de irregularidades y de supuestos de fraude o de corrupción.

La **circunstancia coyuntural favorable** es una creación por parte de las instituciones de la Unión Europea del **instrumento temporal de recuperación NextGenerationEU** que, a través del Plan de Recuperación, Transformación y Resiliencia aprobado por la Comisión Europea, debería acelerar y fomentar el desarrollo de aquellas tendencias.

Por una parte, el instrumento NextGenerationEU aporta un ingente volumen de recursos destinados al desarrollo y la transformación digital del sector público.

Por otra parte, la normativa europea reguladora de aquel instrumento impone a los gestores y beneficiarios de los recursos correspondientes unas obligaciones de integridad especialmente intensas —que, todo sea dicho, deberían de generalizarse a toda la contratación pública Y no exclusivamente aquella financiada con fondos europeos—.

El estudio se estructura en cuatro grandes partes.

En la **primera parte** se estudian en detalle los **elementos contextuales**, estructurales y coyunturales, que acabamos de apuntar, y se analiza el **estado de situación**, tanto en la administración autonómica catalana como en el ámbito local, lo que nos lleva a una constatación: si bien la contratación electrónica ha alcanzado un grado de implantación relevante tanto en la administración de la Generalitat como en los entes locales —cuanto menos en los de más entidad que disponen de más recursos—, la implementación de sistemas automatizados de alerta es todavía absolutamente minoritaria y excepcional.

En este contexto se estudia una iniciativa de gran interés del Consorcio Localret, actualmente en curso, destinado adoptar los entes locales de una herramienta tecnológica de seguimiento, control y planificación de la contratación.

La **segunda parte** del estudio analiza en detalle **tres grandes referentes** de enorme interés: la **herramienta Arachne**, solución tecnológica basada en datos de referencia de la Comisión Europea, que está pone a disposición de toda organización o entidad gestora de fondos europeos como herramienta de lucha antifraude; el **sistema SALER** de la Comunidad Valenciana, pionero en el ámbito que nos ocupa; y el **documento *Red Flags for Integrity***, referencia conceptual, metodológica y práctica inexcusable para el diseño e implementación de sistemas de alerta.

En la **tercera parte**, se desarrollan una serie de reflexiones y consideraciones sobre los sistemas automatizados de alerta, que inciden en la **capacidad preventiva** —más allá de su utilidad contingente— en la medida en que pueden permitir la detección en tiempo real de posibles o potenciales irregularidades, fraudes y supuestos de corrupción, evitando por tanto que lleguen a materializarse.

A continuación se considera la distinción entre **sistemas de alerta internos**, que explotan los datos directamente obtenidos del gestor electrónico de expedientes, y **sistemas externos**, que obtienen los datos de otras fuentes —registros, portales o plataformas de contratación—, lo que nos llevará a la conclusión de la superioridad de los primeros. Asimismo se destaca como los sistemas de alerta sigan de concebir primaria y prioritariamente como una herramienta al servicio de las instancias de control interno, sin perjuicio de otras importantes potencialidades y utilidades que puedan tener.

En tercer lugar se define una **tipología de sistemas de alerta**, basada en las diversas categorías de datos de que se alimentan —datos exclusivamente del procedimiento de contratación que se tramita; del conjunto de la contratación y de la contabilidad de la entidad de que se trate; l los datos anteriores enriquecidos con datos de otras bases de datos y fuentes externas— lo que determina la menor o mayor capacidad de detección de irregularidades, fraudes y corrupción.

Y finalmente, esta tercera parte concluye con un intento de recapitular los **elementos metodológicos** apuntados en este estudio, e intenta ofrecer una síntesis de los elementos básicos y aspectos principales a tener en cuenta. A título ilustrativo, se incluye un cuadro en el que se ha procurado definir los elementos esenciales de las diversas alertas correspondientes a los principales riesgos en el ciclo de la contratación pública.

La cuarta y última parte del estudio contiene las **conclusiones** de cuanto se ha expuesto Y una serie de **recomendaciones** dirigidas a diversos poderes públicos que instituciones.

1 Introducción y consideraciones previas

1.1 Introducción

El año 2017 la Dirección de Prevención de la Oficina Antifraude inició el proyecto *Riesgos para la integridad en la contratación pública*. En el marco de este proyecto, que culmina este año con la publicación, en enero de 2021, del informe final titulado *Compra pública: una cartografía de los riesgos inherentes y de los factores donde enfocar la prevención*, y con la próxima formulación de una serie de recomendaciones preventivas dirigidas a los poderes públicos y a los órganos de contratación, se han generado una serie de documentos y herramientas de gran valor[1], reconocido a nivel nacional e internacional; entre otros

a. 8 documentos técnicos de trabajo dirigidos principalmente a las personas que intervienen en los procedimientos de contratación;

b. una guía interactiva orientada a facilitar el análisis de riesgos en las diversas organizaciones públicas destinatarias; y

c. diversas herramientas y recursos de apoyo a la prevención en este ámbito, así como las aportaciones de personas expertas que analizaron, desde diferentes perspectivas, los riesgos para la integridad en la contratación pública.

Las actuaciones llevadas a cabo por la Oficina Antifraude en el marco de aquel proyecto han consistido, en síntesis, en un exhaustivo y profundo estudio cualitativo de la contratación pública en Cataluña —tal como se indica en la página de presentación del proyecto en la web de la Oficina—.

El presente documento pretende dar continuidad y a la vez complementar aquel estudio cualitativo desde una perspectiva diferente: la perspectiva cuantitativa y tecnológica. Nos proponemos aquí poner el foco de nuestro análisis y reflexión en los **sistemas automatizados de alerta en el ámbito de la contratación pública**.

Como veremos a continuación, la pertinencia y oportunidad de este estudio vienen justificadas por varias circunstancias que convergen en el momento actual, que dan lugar a una interesante ventana de oportunidad:

a. por una parte, como grandes tendencias de fondo, debe mencionarse, en primer lugar, la implantación, cada vez más extendida y profunda, de soluciones informáticas para la tramitación íntegramente electrónica de los procedimientos de contratación pública —lo que responde a un imperativo normativo tanto europeo como nacional—; asimismo, y paralelamente, se observa el progresivo desarrollo e implantación de una cultura y de una gobernanza de los datos, especialmente visibles y

[1] Todos los documentos y materiales son accesibles para su consulta y descarga en la página de presentación del proyecto en la web de la Oficina Antifraude: https://www.antifrau.cat/ca/prevencio/arees-d-estudi/contractacio-publica.

relevantes en el ámbito de la contratación pública, impulsadas y fomentadas por la implantación legal y operativa de los paradigmas de la transparencia y de los datos abiertos; e igualmente, en este contexto, hay que destacar la aparición, en los últimos años, de estudios y propuestas y también de proyectos concretos, cada vez más numerosos, de desarrollo e implantación de sistemas automatizados de alerta basados en el análisis de datos;

b. por otra parte no podemos ignorar un factor acelerador e impulsor, coyuntural y específico de este momento —finales de 2021—: el previsible impulso decisivo a la transformación digital de todo el sector público que deberían representar los fondos provenientes del instrumento NextGeneration EU.

1.2 Sobre el contenido del presente documento

Este estudio no pretende determinar, de manera unívoca y cerrada, cómo tiene que ser y cómo se tiene que configurar un sistema automatizado de alerta.

La razón parece evidente: no existe una solución única; no existe —ni probablemente existirá— una aplicación informática en un lápiz de memoria que, instalada en los servidores de un ente público, garantice la integridad, la conformidad a Derecho, la gestión óptima y la plena corrección de la contratación pública.

Como veremos, las posibilidades y las diversas opciones son prácticament infinitas y la determinación de la solución más adecuada en cada caso requiere un previo análisis y evaluación tanto del contexto normativo y operativo como de los riesgos realmente existentes, que pueden ser muy diferentes en las diversas organizaciones concernidas.

Así pues, lo que aquí se pretende es, en primer lugar, realizar un diagnóstico del estado de situación en el ámbito considerado; en segundo lugar, se pretende plantear una serie de reflexiones y consideraciones, tanto a nivel conceptual como desde el punto de vista metodológico y más operativo, con el objetivo de fomentar la toma de conciencia por todos los poderes públicos de la importancia estratégica de desarrollar e implementar este tipo de sistemas de alerta; finalmente, y en esta línea, se formulan varias recomendaciones dirigidas a los poderes públicos —y también en los operadores privados— a fin de aprovechar y desarrollar al máximo las potencialidades del contexto y del momento concreto en el cual nos encontramos.

Este estudio se concibe pues, más que como el resultado final, definitivo y cerrado, de un estudio sectorial, como un punto de partida, abierto e impulsor —también querríamos que inspirador— de futuros desarrollos, absolutamente necesarios.

El documento se estructura en los apartados siguientes:

a. **diagnosis**: análisis del contexto general —tanto con respecto a las grandes tendencias estructurales como a los factores coyunturales— y de la

situación actual en el ámbito que nos ocupa, tanto a nivel local como autonómico catalán;

b. **referentes**: breve repaso y descripción de algunos referentes más cercanos y de especial interés;

c. **análisis**: reflexiones y consideraciones conceptuales, metodológicas y operacionales; y

d. **conclusiones**: recapitulación y formulación de propuestas y recomendaciones.

1.3 Concepto

La expresión sistema de alerta es polisémica y ambigua. Puede referirse —y, de hecho, en diversos documentos y contexto, se refiere efectivamente— a realidades bastante diferentes:

a. en algunos casos hace referencia a proyectos de análisis de datos de contratación, basados en datos abiertos buen datos obtenidos de plataformas de contratación, a partir de los cuales se generan indicadores de riesgo: este sería el caso, por ejemplo, de Opentender, plataforma de datos de contratación pública del proyecto DIGIWHIST[2]; o del proyecto húngaro Red Flags[3];

b. también se suelen designar como *sistemas de alerta* determinados sistemas basados en el uso de datos masivos que ofrecen en tiempo real —en mayor o menor medida—información para la detección de irregularidades Y Para la evacuación de riesgos: un ejemplo plenamente sería la herramienta Arachne, creada y gestionada per la Comisión Europea[4]; igualmente el sistema SALER de la Inspección General de

[2] El proyecto *DIGIWHIST, The Digital Whistleblower* —digiwhist.eu—, es un proyecto de investigación financiado por la Unión Europea (EU) que se desarrolló entre 2015 y 2018, con la participación de 6 universidades e instituciones de investigación del Reino Unido, Alemania, Hungría, la República Checa e Italia. Uno de los productos del proyecto es la plataforma Opentender —opentender.eu— que recopila datos de licitaciones de 33 jurisdicciones —los 28 estados miembros de la UE, las instituciones europeas, Noruega, Islandia, Suiza y Georgia— de los años 2009 a 2020 y ofrece diversos indicadores —6 indicadores de capacidad administrativa, 10 de transparencia y 7 de integridad—. Los datos utilizados provienen de diversas fuentes pero principalmente de la plataforma de contratación de la Unión Europea TED (*Tenders Electronic Daily*);

[3] El proyecto *Red Flags (Prevention and detection of corrupt procurements through analysis, red flags and follow up*) —www.redflags.eu—, es igualmente proyecto financiado por la Unión Europea en el cual participaron Transparencia Internacional (TI) Hungría, la ONG húngara K-Monitor y PetaByte. Centrado en los datos de contratación húngaros, la web el proyecto aplica a cada uno de los anuncios de licitación y de adjudicación publicados desde 2012 unos indicadores —31 indicadores para los anuncios de licitación y 9 para los anuncios de adjudicación— generadores de alertas indicativas de riesgos en la contratación correspondiente.

[4] De acuerdo con la presentación y el dossier informativo publicados por la Comisión Europea —cfr. nota 51 *infra*—, Arachne es una herramienta tecnológica de minería de datos desarrollada por la Comisión desde 2009 Y plenamente operativo desde septiembre de 2015, puesta disposición de los diversos estados miembros de la UE como herramienta para la prevención de irregularidades, fraude y corrupción en la gestión de los fondos europeos. Como veremos más adelante, la herramienta utiliza datos internos, facilitados por los propios entes gestores y de control de los fondos europeos, y externos, facilitados por dos proveedores externos, Orbis y World Compliance,

Servicios de la Generalitat Valenciana, tal y como aparece descrito en su norma de creación [5], se incluiría esta categoría;

c. pero sistema de alertas también es, indudablemente, un canal de comunicación seguro para alertadores.

En todos estos casos es procedente hablar de alertas: los indicadores de riesgo facilitan información, tanto a escala macroscópica como microscópica, indicativa del nivel de riesgos potenciales y por lo tanto, cuando indican un riesgo elevado, indican una alta probabilidad que se produzca algún tipo de irregularidad; los sistemas en tiempo real alertan, en algunos casos, de irregularidades efectivas o, en otros, de un alto nivel de riesgo en procedimientos concretos; y, como su propio nombre indica, los alertadores ponen en conocimiento de las autoridades de control, internas o externas, situaciones irregulares o incluso de fraude o corrupción de las que puedan tener conocimiento.

Todos son, literalmente hablando, sistemas de alerta; y todos son igualmente necesarios: son las diversas piezas que, junto con otras, integran un sistema de integridad [6].

Sin embargo en este documento nos centraremos en sistemas de alerta basados en datos y procesos de tratamiento automatizado de los mismos.

Los sistemas de alerta que aquí consideramos se podrían pues definir como sistemas tecnológicos que, mediante los correspondientes algoritmos procesan datos de diversas fuentes, tanto intrínsecas a los procedimientos de contratación como extrínsecas a los mismos, detectan y ponen automatizadamente en conocimiento de las instancias de control, internas y/o externas, la existencia o la posibilidad —y, eventualmente, en estos casos, la probabilidad— de irregularidades y, en su caso, impide su efectiva materialización.

---

y ofrece hasta 106 indicadores de riesgo clasificados en 7 categorías. La herramienta Arachne será objeto de un análisis detallado en el apartado 3.1 del presente estudio.

[5] La Ley valenciana 22/2018, de 6 de noviembre, de Inspección General de Servicios y del sistema de alertas para la prevención de malas prácticas en la Administración de la Generalitat y su sector público instrumental, regula el sistema de alerta —conocido como *SALER*, de «Sistema de Alertas Tempranas»— en el Cap. I de su Título II. Trataremos en detalle el sistema SALER en el apartado 3.2 de este estudio.

[6] Desde esta perspectiva amplia, el artículo monográfico *La función de los sistemas de alerta en la gestión de riesgos para la integridad: ¿prevención o contingencia?* de Roger FOLGUERA FONDEVILLA y Lara BAENA GARCÍA, jefe del Área de Generalitat y Parlamento de la Dirección de Investigaciones y consultora de la Dirección de Prevención de la Oficina Antifraude, respectivamente, publicado en el núm. 9, de enero-abril de 2019, de la *Revista Internacional de Transparencia e Integridad* y accesible en: http://www.encuentros-multidisciplinares.org/revista-65/roger-folguera_y_lara-baena.pdf, en el cual se analizan detalladamente los 4 sistemas de alerta a los que se ha hecho referencia —sistema SALER de la Comunidad Valenciana, herramienta Arachne de la Comisión Europea, el sistema MET (*Monitoring European Tender*), derivado del proyecto DIGIWHIST, y proyecto húngaro Red Flags—, incide en sus conclusiones en la necesidad de complementar los *sistemas de alerta* existentes con «las informaciones provenientes de alertadores o *whistleblowers*».

2 Diagnosis

2.1 Contexto general

El mencionado concepto de sistemas automatizados de alerta en el ámbito de la contratación pública, entendido y definido en los términos que acabamos de ver y que en este estudio consideramos, se tiene que situar en un contexto más amplio, que no es otro que el de la **digitalización de la actividad** general **del sector público** y, específicamente, de la actividad de contratación pública.

En los siguientes apartados, repasaremos brevemente el marco normativo en el cual se fundamenta este elemento contextual, los paradigmas que han impulsado su desarrollo y la consecuencia fenomenológica que ha generado.

2.1.1 Marco normativo: procedimiento electrónico y contratación electrónica

Aunque ya existían varios antecedentes normativos —que presentaban, sin embargo, un cierto grado de dispersión y, por lo tanto, planteaban problemas de coherencia entre los diversos regímenes superpuestos—, es la Ley 39/2015, del 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPAC) la que establece los fundamentos y los **elementos esenciales que posibilitan la tramitación electrónica de los procedimientos administrativos**: firma electrónica, registro electrónico de apoderamientos, registro electrónico y notificaciones electrónicas a través del punto de acceso general electrónico de la administración que opera como portal de entrada, sede electrónica, archivo electrónico único de expedientes de procedimientos finalizados; registro de empleados públicos habilitados, etc.

De hecho, la LPAC no se limita a regular estos elementos que posibilitan la tramitación electrónica de los procedimientos; tal como afirma en el apartado III de su exposición de motivos:

> «*... en el entorno actual, **la tramitación electrónica** no puede ser todavía una forma especial de gestión de los procedimientos sino que **debe constituir la actuación habitual de las Administraciones**.*»

Más concretamente, la exposición de motivos de la LPAC, al referirse al título IV de la ley, sobre el procedimiento administrativo común, destaca como la regulación «incorpora a las fases de iniciación, ordenación, instrucción y finalización del procedimiento el uso generalizado y obligatorio de medios electrónicos», y prevé igualmente «la regulación del expediente administrativo estableciendo su formato electrónico y los documentos que deben integrarlo».

La LPAC preveía que los referidos elementos estructurales fundamentales que habían de permitir la existencia y la tramitación, real y efectiva, de procedimientos electrónicos, estuvieran operativos a finales de 2018. Así, la disp. final 7.ª de la LPAC, en su redacción originaria, preveía la entrada en vigor de «las previsiones relativas al registro electrónico de apoderamientos, registro

electrónico, registro de empleados públicos habilitados, punto de acceso general electrónico de la Administración y archivo único electrónico […] a los dos años de la entrada en vigor de la Ley», es decir, el 02/10/2018[7].

La constatación, por parte del legislador, de la imposibilidad de cumplir este plazo por parte de muchas administraciones públicas —especialmente por las administraciones locales—, determinó que la disp. final 7.ª de la LPAC fuera modificada, en un primer momento, por el RD-L 11/2018, de 31 de agosto, de modificación, entre otros, de la LPAC. La nueva fecha de entrada en vigor de sus previsiones relativas al procedimiento electrónico pasaba a ser el 02/10/2020.

Y finalmente, una nueva modificación de la disp. final 7.ª de la LPAC, primero por el RD-L 27/2020, de 4 de agosto, de medidas financieras, de carácter extraordinario y urgente, aplicables a los entes locales, y, al ser revocada aquella disposición por falta de convalidación del Congreso de los Diputados[8], por el RD-L 28/2020, de 22 de septiembre, de trabajo a distancia, que finalmente se convertiría en la Ley 10/2021, de 9 de julio, fijó la fecha de entrada en vigor el 02/04/2021.

Las previsiones normativas no hacen aparecer por sí solas los medios para cumplirlas —especialmente cuando estos medios son tecnológicos y su implantación y puesta en funcionamiento, con los grandes cambios organizativos y operativos que ello comporta, es particularmente compleja—. Y, como veremos más adelante, no se puede afirmar que todas las administraciones hagan un «uso generalizado y obligatorio de medios electrónicos», como pretendía la LCAP.

No obstante, ante la inminencia de la mencionada entrada en vigor de las referidas previsiones de la LCAP, se publicó en el BOE de 31/03/2021 el RD 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos (RAFME), que desarrolla las disposiciones de la LCAP. La exposición de motivos del RAFME incide en la necesidad de «contar con un marco regulatorio adecuado, […], que garantizando la seguridad jurídica para todos los intervinientes sirva a los objetivos de mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada, incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica y garantizar servicios digitales fácilmente utilizables». Y así, al servicio de estos cuatro grandes objetivos —«mejorar la eficiencia administrativa, incrementar la transparencia y la participación, garantizar servicios digitales fácilmente utilizables y mejorar la seguridad jurídica»—, y bajo los principios generales de neutralidad y adaptabilidad a los progresos tecnológicos, de accesibilidad, de facilidad de uso, de interoperabilidad, de proporcionalidad y de personalización y proactividad, proclamados en su art. 2, el RAFME regula detalladamente:

[7] La LPAC fue publicada en el BOE de 02/10/2015, y la disp. final 7.ª preveía su entrada en vigor, con carácter general, al año de su publicación: el 02/10/2016.

[8] Resolución de 10/09/2020, que publica el acuerdo del Congreso de los Diputados por el cual se deroga el RD-L 27/2020, de 4 de agosto.

a. en su título I, los **portales de Internet**, los **puntos de acceso general electrónicos** y las **sedes electrónicas** de las diversas administraciones públicas, así como el **área personalizada** para cada interesado, conocida como ***carpeta ciudadana***;

b. en el título II, el **procedimiento administrativo electrónico** y sus elementos principales: identificación y autenticación, registros electrónicos y notificaciones y comunicaciones electrónicas;

c. en el título III, el **expediente electrónico**, incidiendo en los documentos administrativos electrónicos y su conservación, y en el concepto de archivo electrónico único; y

d. finalmente, en el título IV, la **colaboración** y las **relaciones entre administraciones públicas**, la interconexión de registros —que presupone su interoperabilidad—, la remisión electrónica de expedientes y el intercambio y transmisión de datos.

En Cataluña, el Decreto 76/2021, de 4 de agosto, de Administración digital (DAD) ha retomado y adaptado a las singularidades y especificidades del marco normativo catalán muchas de las disposiciones del RAFME de desarrollo de la LCAP en el ámbito que nos ocupa —hay que tener presente que el RAFME tiene, mayoritariamente, carácter básico, como precisa su disp. final 1.ª—. El DAD, sin embargo, va más allá y, desde una perspectiva más amplia y ambiciosa, incide en el concepto de **gobernanza de los datos**. A este respeto, a su exposición de motivos destaca lo siguiente:

> *«… el régimen jurídico relativo a los medios electrónicos en el ámbito de la Administración de la Generalidad y de su sector público requiere una adaptación a la nueva situación legal y fáctica. Esta adaptación reclama una nueva norma que incorpore* ***no solo las determinaciones necesarias para hacer efectivo el funcionamiento electrónico ordinario****, sino* ***también el modelo de relación y utilización de las nuevas tecnologías*** *más adecuado, eficaz, eficiente, transparente y abierto que sea posible, en atención al marco social y económico sobre el que debe proyectarse.*
>
> *Partiendo de esta necesidad de actualización normativa, la previsión de* ***un gobierno de los datos*** *adecuado debe constituir uno de los pilares fundamentales de aquello que debe ser la Administración digital de la Generalidad. En este sentido, […], es determinante establecer* ***un modelo de datos propio****, en la medida en que la gestión documental y archivística de la información digital se estructura sobre los datos, con el fin de estructurar la documentación administrativa digital de la manera más adecuada.*
>
> ***El gobierno de los datos****, más allá del uso de los datos en el marco de la gestión de los activos digitales,* ***permite crear nuevos servicios digitales analíticos y predictivos*** *utilizando las tecnologías más avanzadas, que son determinantes para la mejora continua de la prestación de los servicios públicos.»*

Consecuentemente, después de establecer en su título I el objeto, el ámbito de aplicación, las finalidades y los principios generales informadores de esta

norma, así como las estructuras organizativas de gobernanza de la Administración digital, el cap. I del título II del DAD regula el **modelo de gobierno de datos**, definido en el art. 10.1 como «el instrumento organizativo que determina los criterios y elementos que definen el gobierno de los datos en la Administración de la Generalidad», el despliegue del cual «se realiza mediante **un protocolo**[9], que es el documento que recoge los aspectos técnicos y organizativos necesarios para implantarlo». Este modelo de gobierno de datos presupone y se fundamenta en una serie de premisas:

a. en primer lugar, que «**Los datos son un *activo digital* compartido** por todos los sujetos [a lo cuales es de aplicación el DAD] […], por lo que **debe maximizarse su reutilización**» —art. 10.2 a) del DAD—;

b. que el modelo de gobierno de datos tiene que ser **común** a pesar de **adaptarse a las necesidades específicas** de cada ente o unidad orgánica —art. 10.2 b)—, incluir «todos los datos fundamentales y todos los datos de las áreas de gestión sectoriales» y ajustarse «a la complejidad de las actividades del área y las necesidades de las personas, según el principio de proporcionalidad» —art. 10.2 c)—;

c. que «La gestión basada en datos se fundamenta en **estándares que garantizan la homogeneidad semántica y sintáctica de las datos**»[10] —art. 10.2 d)— y que «Los datos comunican la información de manera clara y concisa, proporcionando información significativa para facilitar una toma de decisiones» —art. 10.2 e)—;

d. que el modelo de gobierno de datos tiene que garantizar:

   i. «el criterio de **dato único** a través de la colaboración entre los órganos y sistemas custodios de un mismo dato y la identificación unívoca de la fuente más fiable, si procede, en origen» —art. 10.2 f)—, y

   ii. «la **seguridad** de los datos, gestionando su alta, modificación, consulta y borrado de manera segura y con trazabilidad, así como su **autenticidad, integridad, confidencialidad, privacidad y disponibilidad**» —art. 10.2 g)—;

e. finalmente, que el modelo de gobierno de datos tiene que respetar «los principios y requerimientos previstos en el marco de la normativa vigente de **protección de datos, transparencia y acceso a la información, y estadística**», y garantizar «la interoperabilidad y la reutilización» —art. 10.4 del DAD—.

[9] El art. 11 del DAD regula el contenido mínimo del protocolo de gobierno de los datos que ha de incluir los siguientes elementos: «a) Roles y responsabilidades de les personas y organismos que intervienen en el modelo de gestión de los datos. b) Calidad de los datos. c) Ciclo de vida de los datos. d) Modelización y arquitectura de los datos. e) Seguridad. f) Metadatos. g) Catálogo de datos. h) Analítica de datos. i) Sistemas de evaluación y seguimiento del modelo de gobierno de los datos », conceptos, todos ellos, definidos en el glosario del anexo 2 del DAD.

[10] Este concepto de *homogeneidad semántica y sintáctica de los datos* viene igualmente definido en el glosario del anexo 2 del DAD en los términos siguientes: «condición por la que **los datos tienen el mismo significado** para todas las unidades y órganos de la Administración **y se ordenan y se relacionan entre sí de la misma manera**». Se trata, en definitiva, de asegurar que los datos obtenidos y gestionados por una unidad orgánica integrante del modelo puedan ser utilizados con la máxima facilidad, eficacia y eficiencia por cualquier otra unidad.

En definitiva, esta normativa catalana no sólo ha desarrollado las previsiones generales de la LCAP a nivel operativo y procedimental sino que ha definido y establecido un marco conceptual y normativo que establece las bases de una verdadera política de gestión y gobernanza de los datos, alineándose con las mejores prácticas internacionalmente reconocidas [11].

Estos son los principales elementos que integran el marco jurídico general regulador del procedimiento electrónico.

Si consideramos ahora, específicamente, el ámbito de la contratación pública, podemos afirmar que es probablemente uno de los ámbitos de actividad del sector público donde la digitalización se ha desarrollado más intensamente. En ello ha resultado determinante un doble imperativo normativo coincidente:

a. de la normativa europea: Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE

b. de la normativa estatal de transposición de la anterior: la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP).

Cabe destacar, sin embargo, que la digitalización de la actividad de contratación pública ya había empezado mucho antes.

La Generalitat de Cataluña fue pionera en este ámbito: antes, incluso, de la promulgación de la directiva de 2004, reguló, mediante el Decreto 96/2004, de 20 de enero, la utilización de los medios electrónicos, informáticos y telemáticos en la contratación. Este decreto constituyó el marco normativo bajo el cual se empezó a construir el Sistema corporativo de contratación pública electrónica de Cataluña [12], que ha ido integrando los diversos elementos que posibilitaban, de forma gradualmente más y más intensa, la digitalización de la actividad contractual de la Generalitat: registro de licitadores, gestor electrónico de contratación, plataforma de contratación, registro público de contratos, etc.

Por otra parte, constituyó un hito muy relevante, en su momento, la creación, por el art. 42 de la Ley 30/2007, de 30 de octubre, de contratos del Sector Público, del **perfil de contratante** como herramienta de difusión y publicidad en Internet de anuncios, información y datos de contratación pública de las entidades del sector público.

[11] El documento de la OCDE *Analytics for Integrity. Data-driven approaches for enhancing corruption and fraud risk assessments* (OECD, 2019) —accesible en: https://www.oecd.org/gov/ethics/analytics-for-integrity.pdf—, de referencia en el ámbito que nos ocupa, incide reiteradamente en la importancia, para la implementación y desarrollo de cualquier estrategia general o o proyecto concreto basado en datos (*data-driven*), de la existencia de una **cultura y gobernanza de datos** sólidamente implantadas y arraigadas a nivel institucional: «... la efectividad del análisis de datos en cualquier contexto requiere una eficaz gobernanza institucional así como **una buena gobernanza de datos**, datos íntegros y una buena planificación a nivel de proyectos ».

[12] Una descripción de la configuración actual del Sistema y de los elementos que lo integran puede hallarse en: https://contractacio.gencat.cat/ca/contractacio-electronica/.

Pero si la anterior Directiva 2004/18/CE —conocida como directiva *clásica* de contratación pública, la transposición de la cual a nuestro ordenamiento fue precisamente la mencionada Ley 30/2007— apostaba decididamente por el uso intensivo de los medios electrónicos en los procedimientos de contratación, la regulación establecida en la nueva directiva clásica 2014/24/UE representó un verdadero salto cualitativo en este ámbito, en la medida en que preveía, una vez transcurrido un periodo transitorio de 30 meses, **la implantación generalizada de la licitación íntegramente electrónica de los contratos públicos**: el ***e-procurement***, es decir, el uso de los medios electrónicos en todas las fases del procedimiento de contratación[13] —anuncios de licitación, puesta a disposición de los potenciales licitadores de toda la documentación correspondiente, presentación de las solicitudes de participación y de las ofertas, resolución…—. Tal y como indican los apartados (52) y (80) del preámbulo de la Directiva 2014/24/UE, los objetivos son simplificar la publicidad de las licitaciones y hacer los procedimientos de contratación más eficaces y transparentes, facilitando el acceso de los diversos operadores económicos y, especialmente, de las pymes.

La evolución, en este ámbito, de la directiva clásica de 2004 a la vigente de 2014 es muy significativa. Si uno de los objetivos explícitos de la primera era situar en condiciones de igualdad los medios electrónicos y los medios clásicos de comunicación —párrafo (35) del preámbulo—, lo que presuponía que estos últimos eran los medios usuales de comunicación entre operadores económicos y poderes adjudicadores, en la Directiva 2014/24/UE **el uso de medios electrónicos** —definidos en su art. 2.1.19— **deviene la regla general** —art. 22—.

Y tal y como anuncia el párrafo (52) del preámbulo, el art. 90 de la directiva que regula su transposición establece la obligación para todos los Estados miembros de implantar el *e-procurement* previsto en el art. 22 a más tardar el 18/10/2018 —30 meses después de la finalización del plazo de transposición de la directiva, el 18/04/2016.

En este sentido, cabe destacar especialmente las disposiciones de la directiva siguientes:

a. las previsiones relativas a la interoperabilidad —párrafos (55) y (56) del preámbulo— y a la seguridad —párrafo (57) del preámbulo— de los medios electrónicos, así como a la preservación de la integridad y la confidencialidad de los datos, establecidas al art. 22 de la Directiva 2014/24/UE;

b. la obligación para todos los poderes adjudicadores de poner a disposición de los operadores económicos los documentos de licitación —pliegos de cláusulas y demás documentación— por medios electrónicos, en los términos establecidos al art. 53 de la directiva, obligación no sometida al periodo transitorio de 30 meses arriba mencionado y, por lo tanto, en vigor

[13] En palabras de la presentación de la política de *e-procurement* en la página web oficial de la Comisión Europea —accesible en: https://ec.europa.eu/growth/single-market/public-procurement/digital-procurementes—: «La contratación pública está experimentando una transformación digital. La UE apoya el proceso de **repensar el procedimiento de contratación pública teniendo presente las tecnologías digitales**. Esto va más allá de simplemente hacer uso de herramientas electrónicas…».

desde la finalización del plazo de transposición de la directiva, el 18/04/2016, *ex* art. 90.2 *in fine*;

c. la posibilidad, durante el periodo transitorio —y, por lo tanto, antes de la generalización del *e-procurement*—, para aquellos poderes adjudicadores que admitan la licitación electrónica, de reducir los plazos mínimos de presentación de ofertas —arts. 27.4 y 28.5—; y

d. la previsión del art. 59.2 que prevé que el Documento europeo único de contratación (DEUC), que permite a los licitadores acreditar que cumplen los requisitos y criterios de selección cualitativa para poder participar en las licitaciones, sólo podrá facilitarse en formato electrónico.

Como hemos visto, el plazo general de transposición de la directiva clásica de contratación 2014/24/UE finalizaba el 18/04/2016, con la excepción, entre otros, de las previsiones sobre contratación electrónica del art. 22, cuyo plazo de transposición finalizaba el 18/10/2018. No obstante, no fue hasta el 09/11/2017 que se publicó en el BOE la vigente LCSP que transponía finalmente, ya fuera de plazo, la directiva. De acuerdo con su disp. final 16.ª, la LCSP entraba en vigor a los 4 meses de su publicación, es decir, el 09/03/2018, cosa que la exposición de motivos de la ley califica —en un tono quizás excesivamente autocomplaciente— de muestra de «la decidida apuesta [...] [del] nuevo texto legal [...] en favor de la contratación electrónica, estableciéndola como obligatoria en los términos señalados en él, desde su entrada en vigor, anticipándose, por lo tanto, a los plazos previstos a nivel comunitario».

2.1.2 Nuevos paradigmas: transparencia y datos abiertos

El marco normativo que acabamos de describir a grandes rasgos no ha sido, sin embargo, el único factor que ha impulsado el desarrollo de la digitalización de la contratación pública. También han contribuido a ello la progresiva implantación, tanto a nivel legal como operativo, de dos grandes paradigmas íntimamente relacionados: **la transparencia y los datos abiertos**.

En el plano normativo, la introducción de estos paradigmas en nuestro ordenamiento jurídico se produce con la promulgación de las leyes de transparencia: Ley estatal 19/2013, del 9 de diciembre, y Ley catalana 19/2014, del 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno, que imponen a todas las administraciones públicas obligaciones de publicidad activa en materia de organización y estructura administrativa, datos económicos, presupuestarios y de patrimonio, decisiones y actos relevantes, plantilla y puestos de trabajo, procedimientos administrativos, contratos y convenios, subvenciones, informes, planes y programas, y datos estadísticos y geográficos (art. 8 de la Ley 19/2014), previendo explícitamente que los datos sean publicados en el correspondiente Portal de transparencia (art. 5.4 de la Ley 19/2014) en formatos explotables y reutilizables (art. 16 de la Ley 19/2014).

La introducción en nuestro ordenamiento de este régimen de transparencia tiene una importancia primordial y comporta una verdadera revolución, de alcance auténticamente global.

Así, en su obra *Hacia el Derecho Administrativo Global: fundamentos, principios y ámbito de aplicación*[14], los autores, Richard B. STEWART y Benedict KINGSBURY, profesores de la Universidad de Nueva York, identifican los siguientes principios, vertebradores de un nuevo y emergente Derecho público global: el rendimiento de cuentas, la participación, la transparencia, la motivación y el control.

Tres de ellos —los tres, de hecho, profundamente vinculados a la misión de la Oficina Antifraude—, la rendición de cuentas, la transparencia y el control se proyectan sobre y se concretan en lo que se conoce como gobernanza basada en **datos abiertos**. Los imperativos derivados de las leyes de transparencia obligan al sector público a hacer públicos datos sobre su estructura, su funcionamiento y su actividad; estos datos, que son una forma de rendición de cuentas, pueden ser utilizados por la ciudadanía en el marco de los procesos de participación, mejorando y enriqueciendo los procesos de decisión pública y, más generalmente, son considerados un activo intangible de alto valor estratégico —ya hemos visto que así lo explicita el arte. 10.2 a) del DAD: cfr. apartado 2.1.1 anterior.

El carácter y el alcance global de este movimiento es patente si consideramos los diversos documentos internacionales que le dan apoyo.

Así, precisamente el año 2014 el Consejo de la OCDE aprobó la *Recomendación sobre estrategias de gobierno digital*[15] que constituye el primer instrumento legal internacional sobre el gobierno digital. En la presentación de este documento se apunta que «el reto no es la introducción de las tecnologías digitales en las administraciones públicas; es integrar su uso en los esfuerzos de modernización del sector público», y que de lo que se trata es de evolucionar hacia lo «uso de la tecnología para modelar los resultados de la gobernanza pública, y no simplemente para dar soporte a los procesos administrativos de gobierno». Y coherentemente, el apartado II.3 de la recomendación incide en la necesidad de «**crear una cultura basada en datos en el sector público**».

Igualmente, el G20, en su 10.ª cumbre, celebrada en Antalaya (Turquía) en noviembre de 2015, aprobó el documento *Principios de datos abiertos anticorrupción*[16], en cuya nota introductoria se indica lo siguiente:

> *«Estos Principios han sido desarrollados teniendo en cuenta estándares internacionales, buenas prácticas y se fundamentan en tres ideas básicas:*
>
> *1. El progreso exponencial de las tecnologías digitales y el incremento sin precedentes de la cantidad, las fuentes y la calidad de los datos disponibles y de los estándares comunes de datos ofrecen el entorno*

[14] Ed. Derecho Global / INAP, 2016.

[15] *Recommendation of the Council on Digital Government Strategies*, adoptada por el Consejo de la OCDE el 15/07/2014. Accesible en: https://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm.

[16] *G20 anti-corruption open data principles*. Accesible en: http://www.g20.utoronto.ca/2015/G20-Anti-Corruption-Open-Data-Principles.pdf.

adecuado y las herramientas necesarias para promover la disponibilidad y el ***uso de los datos abiertos en la lucha contra la corrupción***.

2. La transparencia es primordial en la lucha contra la corrupción y ambas se pueden reforzar mutuamente a través de una colaboración activa basada en la disponibilidad y el uso de los datos abiertos; y

3. Como tal, los datos abiertos contribuyen a la prevención, la detección, la investigación y la reducción de la corrupción.»

Partiendo de estas premisas, el G20 asumió el conjunto de principios en los cuales se basa la *Carta internacional de Datos Abiertos*[17], que establecen que los datos tienen que ser: abiertos por defecto; actualizados y exhaustivos; accesibles y utilizables; comparables e interoperables; para mejorar la gobernanza y la participación ciudadana; y para el desarrollo inclusivo y la innovación.

El paradigma de la gobernanza basada en datos abiertos se encuentra ya positivizado en nuestro ordenamiento jurídico tanto a nivel europeo como a nivel nacional.

A nivel europeo, la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo del 20 de junio de 2019, relativa a los datos abiertos y la reutilización de información del sector público, cuyo plazo de transposición finalizaba el 17/07/2021, establece un marco normativo mínimo general y formula en su preámbulo (apartados 8.°, 13.°, 14.° y 16.°) las declaraciones siguientes:

«El sector público de los estados miembros recoge, produce, reproduce y difunde una amplia gama de información en numerosos ámbitos de actividad [...]. Los documentos elaborados por los organismos del sector público de carácter ejecutivo, legislativo o judicial constituyen un conjunto amplio, diverso y valioso de recursos, que pueden beneficiar a la sociedad. Ofrecer esta información, que incluye los datos dinámicos, en un formato electrónico de uso habitual permite que los ciudadanos y las personas jurídicas hallen nuevas formas de utilizarla y creen productos y servicios nuevos e innovadores. [...]

La información del sector público o la información recogida, producida, reproducida y difundida en el ejercicio de una misión de servicio público o un servicio de interés general constituye una materia prima importante para diversos productos y contenidos digitales y se convertirá en un recurso cada vez más importante con el desarrollo de tecnologías digitales avanzadas como la inteligencia artificial, las tecnologías de registro descentralizado y el internet de las cosas. [...]

Autorizar la reutilización de los documentos que obran en poder de un organismo del sector público les confiere valor añadido para los reutilizadores, para los usuarios finales y para la sociedad en general y, en muchos casos, para el propio organismo público, ya que el fomento de la

[17] *Open Data Charter*. Accesible en: https://opendatacharter.net/wp-content/uploads/2015/10/opendatacharter-charterF.pdf.

transparencia y la responsabilidad y las aportaciones de reutilizadores y usuarios finales permiten al organismo del sector público de que se trate mejorar la calidad de la información recopilada y la realización de sus misiones de servicio público. […]

*Por **datos abiertos** como concepto se entiende en general los datos en formatos abiertos que puede utilizar, reutilizar y compartir libremente cualquier persona con cualquier fin. Las políticas de apertura de la información […] pueden desempeñar una función importante a la hora de fomentar el compromiso social e impulsar y promover el desarrollo de nuevos servicios basados en formas novedosas de combinar y utilizar esa información.»*

Y a nivel catalán, el gobierno de la Generalitat aprobó el acuerdo GOV/154/2018, de 20 de diciembre [18], por el que se aprueba la estrategia de datos abiertos de la Generalitat de Cataluña y la adhesión a la Carta Internacional de Datos Abiertos.

2.1.3 Marco conceptual: la datificación al servicio de la integridad

En este marco legal y bajo estos paradigmas se ha extendido al sector público el fenómeno conocido como **datificación** [19] de la actividad pública, que podríamos definir como «el proceso de captar todos los aspectos de la vida y transformarlos en datos» [20].

Es notorio que el fenómeno de la datificación se ha producido y extendido en muchos ámbitos de la vida individual y colectiva —social, económica y política— en nuestra sociedad. Pero se produce igualmente —y eso es lo que aquí nos ocupa— en el ámbito de la actividad del sector público.

En la vida privada la datificación es una consecuencia directa del uso cada vez más intensivo de medios electrónicos de comunicación —paradigmáticamente los teléfonos inteligentes que, más allá de permitir comunicarnos, son uno de los principales canales de acceso a las redes sociales y a Internet, y nos permiten llevar a cabo toda clase desde gestiones particulares, económicas, administrativas, financieras o de cualquier otra naturaleza—; este uso genera datos que son masivamente recopilados y explotados por los operadores e intermediarios con que interaccionamos [21].

---

[18] Publicado en el DOGC de 27/12/2018.

[19] Se suele considerar introductores del neologismo *datificación* a Kenneth CUKIER y Viktor MAYER-SCHOENBERGER en su artículo publicado en el núm. de mayo-junio de 2013 de la revista *Foreign Affairs* titulado *The Rise of Big Data* (*La aparición del* Big Data).

[20] Citamos aquí la obra introductoria a la ciencia de datos *Doing Data Science*, de Rachel SCHUTT y Cathy O'NEIL (ed. O'Reilly, 1a ed., octubre 2013; págs. 5 y 6), que recogen la definición del concepto de CUKIER y MAYER-SCHOENBERGER ya analizan críticamente sus implicaciones.

[21] En su obra mencionada —cfr. nota anterior—, SCHUTT y O'NEIL analizan las implicaciones de la datificación en el ámbito privado, observando al respecto:

a. per una parte, que «la datificación es un concepto interesante que nos lleva a considerar su importancia en relación con la intencionalidad de la gente a la hora de compartir sus propios datos », destacando que no siempre asumimos conscientemente y voluntariamente que

En el sector público, reencontramos este mismo fenómeno, que se extiende cada vez más rápida e intensamente, impulsado por las dos fuerzas que hemos mencionado hasta aquí:

a. por una parte, directamente, la tramitación electrónica de los procedimientos administrativos comporta la generación directa de datos almacenados —de forma más o menos automatizada y más o menos fácilmente recuperables y, por lo tanto, explotables— en el propio expediente electrónico y los documentos electrónicos que lo integran, así como, eventualmente, en las aplicaciones de gestión que soportan y facilitan la tramitación;

b. por otra parte, indirectamente, los imperativos derivados tanto de la transparencia como de la progresiva implantación y desarrollo del paradigma de los datos abiertos obligan los organismos y entidades del sector público a recopilar en *soportes electrónicos* determinados datos —los que tienen que ser objeto de publicidad activa, como a mínimo—, incluso si estos datos no se encuentran en un expediente o documento electrónico.

Tanto en un caso como en el otro, el resultado final es que cada vez la actividad del sector público genera más datos en soportes electrónicos y, por lo tanto, fácilmente recopilables, almacenables, tratables y explotables para muy diversas finalidades. Paralelamente, la última década ha visto incrementarse exponencialmente las capacidades técnicas de almacenamiento y de explotación de esta ingente cantidad de datos, con un coste cada vez más reducido.

Las finalidades al servicio de las cuales se puede poner esta capacidad exponencialmente creciente de recopilación, almacenaje y análisis de los datos generados por el sector público son múltiples:

a. tradicionalmente —en el sector privado mucho antes que en el público— el análisis de datos ha servido en primer lugar como herramienta al servicio de la **toma de decisiones** de gestión operativa o estratégica;

b. estrechamente vinculada a la anterior —de hecho, es una concreción de la misma—, otra finalidad es la o**ptimización del uso de recursos limitados**: el conocimiento y la eventual previsión, sobre una base empírica y cuantitativa, de los efectos y del impacto de las decisiones de asignación de los recursos disponibles permite evaluarlas y, en una dinámica cíclica —como sería, por ejemplo, la de los procesos anuales de elaboración presupuestaria—, optimizarlas;

---

muchas de nuestras acciones en contextos y a través de medios electrónicos sean datificadas;

b. y, consiguientemente, cuestionando las consecuencias y corolarios que CUKIER y MAYER-SCHOENBERGER extraen de la definición de datificación —«Una vez que hemos datificado las cosas, podemos transformar su utilidad convirtiendo la información en nuevas formas de valor»—, afirman que hay que interrogarse sobre quién lleva a cabo esta transformación, cuáles son estas nuevas formas de valor, y, obviamente, quién se beneficia de ellas.

c. más recientemente, el uso de herramientas de análisis masivo de datos y de aprendizaje automático se está utilizando para **personalizar proactivamente los servicios públicos electrónicos** ofrecidos a la ciudadanía [22];

d. y, evidentemente, la datificación del sector público tiene que ponerse, inexcusablemente, **al servicio de la integridad**, permitiendo y facilitando la prevención, detección, corrección y persecución de irregularidades y, en su caso, de supuestos de fraude y/o de corrupción.

Esta idea de poner la datificación del sector público al servicio de la integridad constituye el núcleo de un documento que podemos considerar una referencia esencial en este ámbito: el documento de la OCDE *Analytics for Integrity. Data-driven approaches for enhancing corruption and fraud risk assessments (Herramientas analíticas para la Integridad. Aproximaciones basadas en datos para una mejor evaluación del riesgo de fraude y corrupción)* [23].

El documento parte de los principios, buenas prácticas y metodologías clásicas de evaluación de riesgos y constata que el «advenimiento de la edad digital en el gobierno ha generado nuevas oportunidades para la evaluación de los riesgos de fraude y corrupción», contraponiendo las **técnicas o aproximaciones cualitativas** de evaluación de riesgos de fraude y corrupción, basadas en percepciones humanas de los sujetos implicados —y, correlativamente, en su sensibilización y formación—, con las **aproximaciones cuantitativas**, basadas en los datos y en la utilización de herramientas analíticas [24], y destaca reiteradamente que **las aproximaciones cualitativas y cuantitativas son recíprocamente** complementarias [25].

---

[22] La *Recomendación sobre estrategias de gobierno digital* de la OCDE de 2014, ya citada —cfr. nota 15 anterior—, destaca en su introducción precisamente la conveniencia para los poderes públicos de «reorganizarse en torno a las expectativas, necesidades y requisitos asociados de los usuarios [de los servicios públicos], más que centrándose en sus propias lógicas y necesidades».

Y de hecho el art. 4 c) del DAD enumera entre los principios generales de la administración digital precisamente el de «Proactividad y personalización en la prestación de servicios públicos digitales con el objetivo de situar la experiencia de las personas en el centro del diseño de servicios».

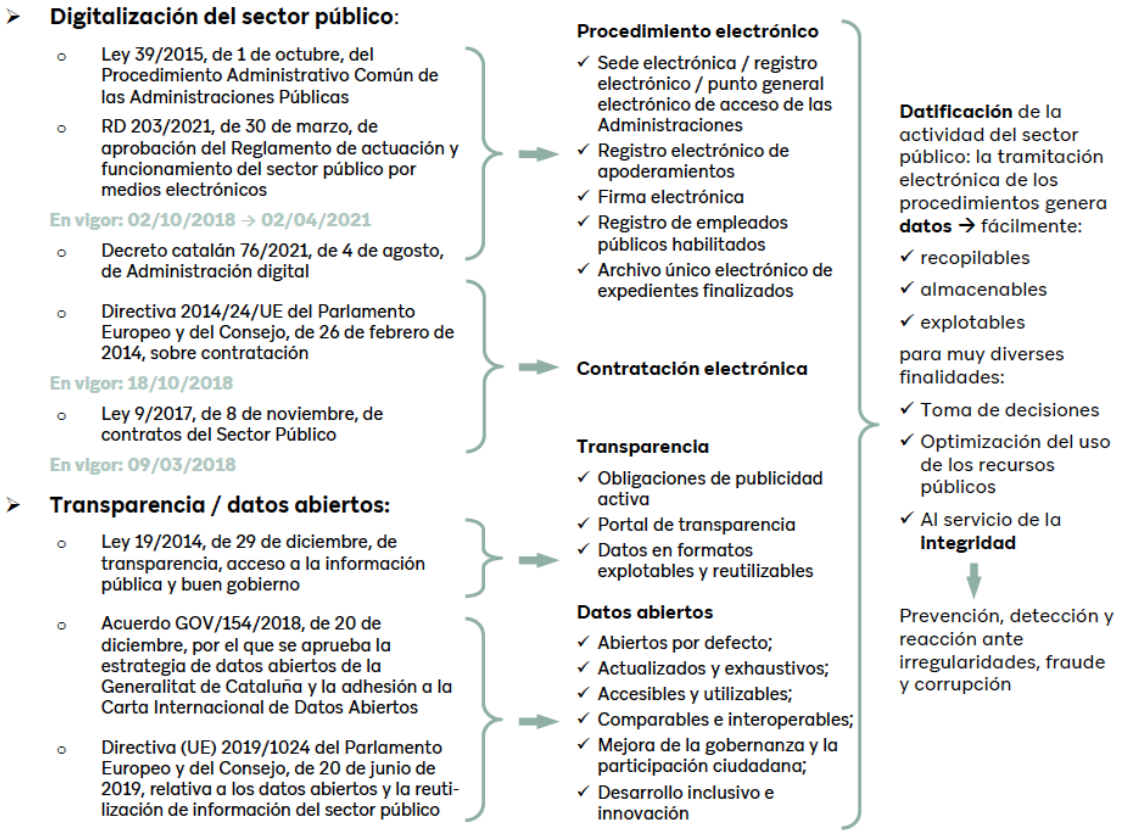
[23] Cfr. nota 11 anterior.

[24] *Op. cit.* pág. 7: «... los gestores de proyectos, los gestores de riesgos, los responsables de contratación y los órganos de control, entre otros, se basan a menudo en **metodologías cualitativas** de evaluación de riesgos [de fraude y corrupción] (p. ej. encuestas y entrevistas para la identificación y ponderación de los riesgos). El resultado paradigmático de estas aproximaciones basadas en percepciones son los inventarios y mapas de riesgos que muestran la magnitud y la probabilidad de los riesgos percibidos. Estas aproximaciones pueden facilitar una comprensión de los riesgos más críticos y constituyen un medio efectivo para implicar a las personas de una organización en la gestión de riesgos. [...]el a**nálisis de datos** puede complementar las metodologías cualitativas, e incrementar la comprensión de los riesgos existentes por parte de los gestores y permitir la toma de decisiones basadas en datos objetivos para la mitigación de los riesgos.»; y pág. 17: «No existe una metodología uniforme de evaluación de riesgos, pero las aproximaciones pueden ser, en general **cualitativas, cuantitativas o mixtas**. [...] los **métodos cuantitativos** que utilizan el análisis de datos para evaluar los riesgos dependen de la disponibilidad y la calidad de datos y requieren sólidas técnicas de análisis.».

[25] *Op. cit.* pág. 18: «Cuando los datos están disponibles, son fiables y válidos, los métodos cuantitativos de evaluación de riesgos y la aplicación de técnicas analíticas pueden contribuir a complementar la evaluación cualitativa implantada en una organización».

Partiendo de esta premisa, se exponen y analizan los pasos a seguir para la «creación de un plan de análisis de datos con objetivos específicos de integridad y la selección de las técnicas más adecuadas de acuerdo con estos objetivos y los recursos disponibles». A partir de la experiencia concreta del desarrollo de un proyecto basado en datos de evaluación y gestión de riesgos en grandes proyectos de infraestructuras en el Grupo Aeroportuario de la Ciudad de México, en el cual colaboró la OCDE, se destacan la metodología a seguir, los elementos claves, las mejores prácticas y los resultados obtenidos.

Sintetizando todas estas ideas en un esquema, tendríamos el siguiente:



2.2 El cisne negro: los fondos NextGenerationEU

Se suele designar como *cisne negro* un acontecimiento que reúne tres características: es totalmente imprevisto y atípico, fuera del ámbito de las expectativas razonables; es disruptivo en tanto que tiene un impacto socioeconómico extremo; y, a pesar de su rareza, es retrospectivamente explicable y racionalizable[26].

Este concepto resulta bastante adecuado para describir la decisión de las instituciones de la UE de crear, a finales de 2020 y principios de 2021, el instrumento temporal de recuperación NextGenerationEU, dotado con 806.900 millones de euros, destinado, junto con el presupuesto a largo plazo de la UE

[26] Este concepto de *cisne negro* se suele atribuir al filósofo e investigador Nassim Nicholas TALEB, descrito y desarrollado en su libro *The Black Swan. The Impact of Highly Improbable* (*El cisne negro. El impacto de lo muy improbable*), Random House, 2.ª ed. 2010.

2021-2027, a hacer frente a la crisis generada por la COVID-19 y a fomentar la transición hacia una Europa más moderna, sostenible y resiliente [27].

No es este el lugar adecuado para estudiar en profundidad este instrumento, pero sí que consideraremos brevemente dos aspectos de lo mismo: los recursos destinados en nuestro país a profundizar y desarrollar la digitalización de las administraciones públicas, por un lado, y, por otro, las exigencias en materia de integridad que tienen que cumplir todos los beneficiarios de aquellos fondos.

2.2.1 Recursos

La principal componente del instrumento NextGenerationEU es el Mecanismo de Recuperación y Resiliencia (MRR), establecido por el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021.

En el marco del MRR, el Gobierno del Estado aprobó el 27/04/2021 el Plan de Recuperación, Transformación y Resiliencia (PRTR) [28] que, una vez enviado a la Comisión Europea, fue aprobado por ésta el 16/06/2021.

El PRTR se estructura alrededor de cuatro ejes transversales, uno de los cuales es el de *Transformación Digital*. Estos ejes orientan las 10 *políticas palanca* [29] que articulan las 30 componentes concretas que integran el Plan. La cuarta política palanca, bajo el título *Una Administración para el siglo XXI*, incluye una única componente, la 11.ª, denominada: *Modernización de las Administraciones Públicas*.

El PRTR prevé una inversión pública del orden de 70.000 millones de euros en el periodo 2021-2023, estructurada en 20 *programas tractores de inversión* [30], el tercero de los cuales, por orden de magnitud, es el correspondiente a la mencionada componente 11.ª, de *Modernización de las Administraciones públicas*, con un presupuesto total para los ejercicios 2021 a 2023 de 4.239 millones de euros.

En el documento complementario de desarrollo de esta componente 11.ª del PRTR, se especifican los objetivos estratégicos que incluyen la «digitalización de la Administración y procesos», la «modernización de las Administraciones Públicas, incluyendo […]un refuerzo del marco de contratación pública», y el

[27] Una explicación global y detallada puede hallarse en el documento publicado en abril de 2021 por la Comisión Europea: *The EU'S 2021-2027 long-term Budget and NextGenerationEU. Facts and Figures*. Accesible en: https://op.europa.eu/es/publication-detail/-/publication/d3e77637-a963-11eb-9585-01aa75ed71a1/language-en.

[28] El PRTR, la documentación complementaria y de desarrollo del mismo y el resto de documentación e información relacionadas están accesibles en: https://planderecuperacion.gob.es/documentos-y-enlaces.

[29] En palabras del PRTR, los 4 ejes transversales —transición ecológica, transformación digital, cohesión territorial y social e igualdad de género— «se proyectan en 10 políticas palanca, de gran capacidad de arrastre sobre la actividad y el empleo […], para impulsar la recuperación económica a corto plazo y apoyar un proceso de transformación que aumente la productividad y el crecimiento potencial de la economía española en el futuro.» (PRTR, versión de 16/06/2021, pág. 24).

[30] PRTR, versión de 16/06/2021, pág. 34.

«refuerzo de las capacidades administrativas». Entre los programas concretos de reformas y de inversión de esta componente, hay que destacar los siguientes:

a. el programa de reforma C11.R4, centrado en la implementación efectiva de la Estrategia Nacional de Contratación Pública —por cierto ya prevista y regulada en el art. 334 de la LCSP— y que incide, entre otros aspectos, en la «transformación digital de la contratación pública», entendida como «impulso coordinado para culminar la plena extensión de la utilización de la contratación pública electrónica»;

b. el programa de inversiones C11.I1, de modernización de la Administración General del Estado, que entre otras actuaciones prevé el desarrollo de «herramientas que permitan digitalizar el flujo de la tramitación de los expedientes de contratación, así como herramientas basadas en analítica de datos e Inteligencia Artificial que faciliten la gestión de los servicios» mediante una iniciativa singular de *e-procurement*; y

c. el programa de inversiones C11.I3, de transformación digital y modernización de las Administraciones autonómicas y locales; este programa prevé unos recursos totales de 578,6 millones de euros para las Comunidades Autónomas y de 391,4 millones de euros para los entes locales, con los cuales se financiarán proyectos de modernización alineados con la Estrategia Digital 2025 [31] y el Plan de Digitalización de la Administración Pública [32], orientados, entre otros, al desarrollo de «herramientas que permitan digitalizar y homogeneizar la tramitación de los expedientes y procesos de contratación pública para cubrir el proceso de contratación de principio a fin, así como ayudar en la toma de decisiones mediante la analítica de datos y la automatización inteligente, fomentando el *e-procurement*».

Destaquemos finalmente que mediante la Orden TER/1204/2021, de 3 de noviembre, publicada en el BOE de 06/11/2021, se aprueban las bases reguladoras y se convocan las subvenciones correspondientes a este último programa de inversión. En la exposición de motivos de dicha disposición se indica que de los 391,2 millones de euros del programa están disponibles 92,77 en el presente ejercicio 2021, con los cuales se subvencionarán proyectos de transformación digital y modernización de las administraciones de las entidades locales de más de 50.000 habitantes o menos que sean capitales de provincia —art. 1.1 de la orden— hasta el importe máximo asignado a cada entidad en el anexo V de la orden —art. 9.3 y .4—.

En el ámbito catalán, el Gobierno de la Generalitat aprobó el documento *Next Generation Catalonia*, que recoge los proyectos catalanes que optan a la

[31] La agenda España Digital 2025, presentada por el Gobierno del Estado el 23/07/2020, está accesible en: https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx.

[32] El Plan de Digitalización de las Administraciones Públicas 2021-2025, del que se informó en el Consejo de Ministros del 26/01/2021, es accesible en: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Estrategia-TIC/Plan-Digitalizacion-AAPP.html#.Ybsq_y0rz-Y.

financiación de los fondos NextGenerationEU en el marco del PRTR[33]. El proyecto 17.° de los 27 incluidos en el mencionado documento se enmarca en el eje estratégico E.3, *Transformación Digital*, y el ámbito de actuación A.15, *Transformación de las Administraciones Públicas*, tiene un presupuesto de 210 millones de euros para su primer año de ejecución de un total de 1.120 millones, y prevé como actores implicados en su definición y ejecución la Generalitat de Cataluña, el Consorcio AOC, el Consorcio Localret, las Diputaciones y las universidades catalanas, entre otros.

2.2.2 Requisitos de integridad

Es notorio que la ejecución de un volumen tan importante de recursos públicos plantea importantes retos a todos los niveles de las administraciones gestoras y beneficiarias de los fondos NextGenerationEU.

Para establecer el marco regulador correspondiente, se publicó en el BOE del 30/09/2021 la Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del PRTR. De acuerdo con su art. 1.1, esta orden «configura y desarrolla un Sistema de Gestión orientado a definir, planificar, ejecutar, seguir y controlar los proyectos y subproyectos en que se descomponen las medidas (reformas/inversiones) previstas en los componentes del Plan de Recuperación, Transformación y Resiliencia», y enuncia los principios o criterios de gestión que han de informar este sistema —art. 2.2—, entre los cuales cabe destacar, a los efectos que aquí nos interesan, el «refuerzo de mecanismos para la prevención, detección y corrección del fraude, la corrupción y los conflictos de interés», principio que se concreta en el art. 6 que prevé específicamente, entre otros aspectos:

a. que «toda entidad, decisora o ejecutora, que participe en la ejecución de las medidas del PRTR tendrá que disponer de un "Plan de medidas antifraude" que le permita garantizar y declarar que, en el su respectivo ámbito de actuación, los fondos correspondientes se han utilizado de conformidad con las normas aplicables, en particular, en lo que se refiere a la prevención, detección y corrección del fraude, la corrupción y los conflictos de interés» —art. 6.1—;

b. a estos efectos, la obligación para todos los órganos gestores de llevar a cabo una evaluación de los riesgos de fraude —art. 6.4, primer inciso—;

c. la elección de las medidas de prevención y detección adecuadas, a juicio de cada órgano gestor, atendiendo a sus características específicas —art. 6.4, segundo inciso—;

d. como concreción de todo el anterior, la aprobación, en un plazo inferior a 90 días desde la entrada en vigor de la orden o desde que se tenga

[33] El documento *Next Generation Catalonia* fue aprobado por el Gobierno de la Generalitat el 02/02/2021, juntamente con el DL 5/2021, de 2 de febrero, de medidas para la implementación y la gestión de los fondos del Mecanismo de Recuperación y Resiliencia de la UE.

Puede accederse a información sobre dicho documento en: https://territori.gencat.cat/ca/detalls/Article/projectes-tes-00001, y al documento en sí en: http://economia.gencat.cat/web/.content/20_departament_gabinet_tecnic/arxius/pla-recuperacio-europa/next-generation-catalonia.pdf.

conocimiento de la participación en la ejecución del PRTR, de un Plan de medidas antifraude (PMA) con el contenido y requerimientos mínimos establecidos en el apartado 5 del art. 6 de la orden; y

e. las actuaciones a llevar a cabo en caso de detección de un posible fraude o de que se tenga de ello una sospecha razonable —art. 6.6 y .7—.

Cabe destacar que estas previsiones no hacen otra cosa que transcribir en una disposición reglamentaria estatal una serie de disposiciones del Derecho europeo que no son nada nuevas, dado que son aplicables a la gestión de los fondos europeos desde hace como mínimo 15 años[34]. En este sentido, no deja de resultar paradójico que la adopción de medidas antifraude sea —de hecho, haya venido siendo, dado que la normativa europea era de directa aplicación— una **obligación** en la **gestión de recursos públicos de la UE** —y, concretamente, en la contratación financiada con fondos europeos— pero **no lo haya sido** —y, de hecho, siga sin ser obligatoria— cuando de la gestión y contratación financiada con **recursos de las haciendas nacional, autonómicas o locales** se trata.

Para facilitar el cumplimiento de estas disposiciones, y «lograr una homogeneidad en el diseño de estas medidas [antifraude] […], y sin perjuicio de la aplicación de medidas adicionales atendiendo a las características y riesgos específicos de la entidad de qué se trate» —art. 6.2—, la orden facilita, por una parte, en su anexo II.B.5, un «Test [de] conflicto de interés, prevención del fraude y la corrupción» destinado a facilitar la autoevaluación de riesgos y medidas existentes por parte de las diversas entidades concernidas, y, por otra parte, en su anexo III.C, una serie de orientaciones sobre posibles medidas a adoptar. Entre las posibles medidas antifraude a las cuales hace referencia la orden, nos interesan especialmente las relativas a mecanismos basados en datos:

a. el test de autoevaluación de riesgos y medidas existentes contiene una única pregunta sobre esta cuestión, la 10.ª: «¿Se utilizan herramientas de prospección de datos o de puntuación de riesgos?», lo que indica que, a la hora de evaluar los riesgos, se atribuye a este aspecto una importancia bastante relativa —representa un máximo de 4 puntos sobre una puntuación máxima total de 64—;

b. las orientaciones del anexo III.C contienen algunas referencias más:

[34] Ya en 2006, el Reglamento (CE) 1083/2006, del Consejo, de 11 de julio de 2006, que establecía las disposiciones generales comunes a los fondos europeos (FEDER, Fondo Social Europeo, Fondos de Cohesión, etc.) imponía a los Estados miembros, en su art. 70.1, la obligación de «prevenir, detectar y corregir las irregularidades y recuperar los importes indebidamente abonados». Para facilitar el cumplimiento de esta obligación la Comisión Europea publicó la Nota informativa COCOF/0003/00, sobre indicadores de fraude, que formaba parte de la Estrategia Conjunta de Prevención del Fraude puesta en marcha en 2008.

Posteriormente, el art. 125.4 c) del Reglamento (UE) 1303/2013, del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, que derogó y substituyó el anterior, estableció mucho más explícita y claramente la obligación de «aplicar medidas antifraude eficaces y proporcionadas, teniendo en cuenta los riesgos detectados» y a estos efectos la Comisión Europea publicó la Nota orientativa EGESIF/14/0021/00, de 16/06/2014, sobre evaluación del riesgo de fraude y medidas antifraude efectivas y proporcionadas.

Las previsiones de la Orden HFP/1030/2021, de 21 de septiembre, básicamente transcriben parte del contenido de aquella normativa y documentación europea.

i. en lo atinente a la prevención de los conflictos de intereses —apartado 1 d) i.C—, se hace referencia explícitamente a la «comprobación de información a través de bases de datos de los registros mercantiles, bases de datos de organismos nacionales y de la UE, expedientes de los empleados (teniendo en cuenta las normas de protección de datos) o a través de la utilización de herramientas de prospección de datos («*data mining*») o de puntuación de riesgos»;

ii. en lo relativo a la prevención y la detección del fraude —apartados 2 b) i.G y 2 b) ii.A—, se hace referencia, para la prevención, al «análisis de datos», entendido como «dentro de los límites relativos a la protección de datos, cruce de datos con otros organismos públicos o privados del sector que permitan detectar posibles situaciones de alto riesgo incluso antes de la concesión de los fondos»; y para la detección, al «uso de bases de datos como la Base Nacional de Datos de Subvenciones (BNDS), herramientas de prospección de datos («*data mining*») o de puntuación de riesgos».

Como puede verse, las soluciones basadas en datos y análisis de datos, si bien aparecen mencionadas como posibles elementos constitutivos de los PMA que la orden exige a todos los órganos y entidades decisores o ejecutores de medidas o acciones del PRTR, no constituyen uno de sus elementos centrales, más bien aparecen con un cierto carácter residual.

Ahora bien, el ya mencionado documento de la OCDE *Analytics for Integrity* [35] apunta una idea muy interesante: tratando de determinar la relación de beneficios por inversiones en sistemas basados en datos y análisis de datos, cuantificada en términos de eficacia en la reducción del fraude, hace referencia a un estudio llevado a cabo en el año 2016 por la Asociación de Examinadores de Fraude Certificados (ACFE por sus siglas en inglés) que demuestra que los sistemas de monitorización y análisis de datos son los que permiten la mayor reducción de pérdidas por fraude respecto de otros 18 mecanismos de control y detección —códigos de conducta, protección de alertadores, auditorías externas por sorpresa, estados financieros, etc. —. En el apartado de este estudio dedicado a la efectividad de los controles antifraude [36] se indica que:

> *«… medir el valor preventivo de los controles concretos es extremadamente difícil, si no imposible. Aun así, los profesionales antifraude a menudo han de presentar argumentos a los gestores con el fin de obtener recursos adicionales para hacer frente a los riesgos de fraude. Para ayudar a ilustrar la rentabilidad de los controles antifraude concretos, hemos examinado la media comparada de pérdidas por fraude y el tiempo de detección de fraudes en las organizaciones en función de cada uno de los 18 controles antifraude existentes en el momento en que se produjo el fraude.»*

[35] Op. cit. pág. 39. Cfr. notas 11 y 23 anteriores.

[36] *Report to the Nations on Occupational Fraud and Abuse. 2016 Global Fraud Study* (ACFE, 2019) págs. 43 y 44. Accesible en: https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf.

y los cuadros comparativos correspondientes ponen de manifiesto que **la monitorización proactiva y el análisis de datos constituye el mecanismo de control que más reduce las pérdidas por fraude** —reducción del 54,0%— de los 18 controles posibles considerados.

Así pues, y con base en este estudio, la apuesta por mecanismos de prevención y detección del fraude basados en datos y análisis de datos parece ser de las más interesantes, en términos de eficacia.

2.3 Situación

Hasta aquí hemos repasado lo que *tendría que ser* —el marco normativo— y lo que *tendría que llegar a ser* —las perspectivas de futuro que abren los fondos NextGenerationEU—. ¿Pero cómo es la realidad, lo que *es*? ¿Cuál es la situación real de la digitalización de la contratación pública en Cataluña y de los sistemas automatizados de alerta que puedan existir?

2.3.1 Generalitat de Cataluña

La Generalitat de Cataluña cuenta, desde hace más de 10 años con una solución tecnológica para la tramitación electrónica de expedientes de contratación: el **Gestor electrónico de expedientes de contratación (GEEC)**[37].

El GEEC se empezó a desarrollar en 2006 en virtud de un encargo, aprobado por acuerdo del Gobierno de 05/09/2006, al Departamento de Economía y Finanzas, a través de la Junta Consultiva de Contratación Administrativa y con la colaboración del Centro de Telecomunicaciones y Tecnologías de la Información (CTTI). El objetivo era la creación de una herramienta de tramitación electrónica de los expedientes de contratación de los departamentos de la Administración de la Generalitat y de los entes públicos dependientes o vinculados a los mismos.

La versión inicial del GEEC fue aprobada por Orden ECF/193/2008, de 29 de abril, y se desplegó escalonadamente en todos los Departamentos de la Generalitat y algunas entidades con gran volumen de contratación en 2008.

En abril de 2017 se aprobó el inicio de una profunda renovación tecnológica del GEEC, que dio lugar al GEEC 2.0, con un cambio de tecnología —se pasó del entorno SAP original a una solución web, con una arquitectura modular basada en microservicios que permite sustituir piezas de forma independiente en caso de necesidad, facilitando la evolución tecnológica progresiva del sistema—, un entorno más usable, intuitivo, flexible y escalable, una reducción de costes de desarrollo, mantenimiento, implantación y formación, y la adaptación de la herramienta a las modificaciones del marco legal derivadas de la entrada en vigor de la LCSP de 2017.

[37] Se puede acceder a la información sobre el GEEC, a su normativa reguladora y a los datos de su uso en la página web oficial de la Generalitat de Cataluña: https://contractacio.gencat.cat/ca/gestionar-contractacio/contractacio-electronica-administracio/geec/.

El GEEC 2.0 fue aprobado por la Orden VEH/159/2020, de 21 de septiembre, que regula y describe sus características esenciales:

a. de acuerdo con el art. 2.1 de la orden, es mediante el GEEC que «los departamentos de la Administración de la Generalitat y los entes del sector público que dependen o se hallan vinculados a los mismos, **deben tramitar la totalidad de su contratación pública**, con independencia de la tipología de expedientes y de los procedimientos, formas e instrumentos utilizados para su adjudicación», con la única exclusión de «los gastos que, en razón de su naturaleza y cuantía y previamente autorizados por los órganos competentes, se tramitan en concepto de mandamiento de pago a justificar»; el mismo precepto prevé igualmente que puedan hacer uso del GEEC «los organismos independientes y estatutarios que lo soliciten»;

b. el art. 3.2 enumera los **módulos** de que consta el GEEC, que son los siguientes:

   i. el «módulo básico de gestión y de seguimiento de expedientes», que permite el inicio del expediente de contratación por la unidad promotora, la tramitación hasta las fases de ejecución, resolución y liquidación del contrato, la anexión y generación de documentos a partir de plantillas preestablecidas y personalizables, la firma y copia auténtica de los documentos, la visualización de las fases, trámites y tareas del expediente mediante un árbol de tramitación interactivo, con trazabilidad del histórico de acciones realizadas, la consulta del expediente, la generación de «alertas y avisos sobre el proceso de tramitación», la emisión de informes operativos, la clasificación archivística de los documentos y generación del fichero de archivo del expediente, la tramitación excepcional y masiva de expedientes y la exportación de información para su carga en cuadros de mando o herramientas de análisis de información propias de las entidades o de la Intervención General;

   ii. el «módulo de visor del expediente, para personas no usuarias de la herramienta de tramitación que han de acceder al expediente […] para llevar a cabo las tareas de generación y fiscalización de apuntes contables», que permite la búsqueda de expedientes, la consulta de los datos básicos, de tramitación y documentación del expediente, y funciones de exportación de un expediente para su posterior remisión;

   todo ello sin perjuicio de posibles nuevas funcionalidades que se puedan ir incorporando, así como de otros módulos en función de nuevas necesidades que se puedan plantear;

c. el art. 2.2 de la orden incide en un elemento importante: **la integración del GEEC con los sistemas económicos y financieros** corporativos de la Generalitat de Catalunya, y, en esta línea, el art. 4.3 prevé la integración del GEEC con los sistemas económicos financieros y los cuadros de mandos departamentales o propios de los entes públicos, y el art. 4.1 prevé expresamente la integración del GEEC con las aplicaciones corporativas de la Generalitat de Cataluña y los sistemas de información de otras administraciones vinculados a la contratación pública, haciendo referencia, entre otros, en los siguientes:

i. el sistema económico financiero corporativo de la Generalitat de Cataluña (GECAT y Pangea);

ii. el punto general de entrada de facturas electrónicas del Consorcio AOC (eFact);

iii. el Registro público de contratos (RPC);

iv. el Registro electrónico de empresas licitadoras y clasificadas (RELI);

v. las aplicaciones corporativas de autenticación de usuarios, de firma electrónica, de digitalización y copia auténtica de documentos, y de validación de firmas;

vi. la Plataforma de Servicios de Contratación Pública (PSCP);

vii. la plataforma de archivo de documentos electrónicos del Consorcio AOC (iArxiu);

viii. la herramienta de recepción de ofertas electrónicas (Sobre digital);

ix. la plataforma de notificaciones electrónicas (eNotum);

x. los sistemas de la AEAT, la TGSS y la ATC.

Los datos de uso del GEEC [38] indican una utilización creciente: si en el 2020 lo utilizaban 41 órganos de contratación, con 2.692 usuarios, en septiembre de 2021 son 52 órganos de contratación con 3.054 usuarios.

Paralelamente, la Generalitat de Cataluña cuenta con otra herramienta: el **Tramitador electrónico de expedientes de contratación (TEEC)** [39], dirigido a las unidades de contratación del sector público de la Generalitat y de los entes estatutarios que no dispongan del GEEC, así como a los entes locales.

El TEEC fue aprobado por la Orden ECO/295/2015, de 18 de septiembre, que, en su exposición de motivos, lo presenta como «la herramienta que tiene que facilitar e impulsar la gestión electrónica de los expedientes de contratación para las entidades del sector público de la Generalitat con un determinado perfil de contratante que, de acuerdo con los criterios objetivos de eficiencia, requieren un sistema de información específico y simplificado con respecto a lo que supone [...] la herramienta corporativa del GEEC».

El TEEC, que igual que el GEEC 2.0 es una herramienta de acceso vía web, presenta sin embargo algunas diferencias relevantes respecto del GEEC, que se desprenden de su regulación y descripción en la mencionada orden de aprobación del mismo:

a. en primer lugar, tal como precisa el art. 1.2 de la orden, la aplicación TEEC «está **basada en productos de mercado**, sobre los cuales se han

[38] Datos actualizados a septiembre de 2020. Cfr. nota anterior.

[39] Se puede acceder a información sobre el TEEC, a su normativa reguladora y a los datos de uso en la página web oficial de la Generalitat de Cataluña: https://contractacio.gencat.cat/ca/gestionar-contractacio/contractacio-electronica-administracio/teec/.

incorporado funcionalidades a medida [...]. Todo el software reside en las instalaciones del proveedor de servicios de la Generalitat»;

b. con respecto a las entidades a las cuales va destinado, el art. 2 distingue:

   i. por una parte las «entidades del sector público de la Administración de la Generalitat, incluyendo las universidades catalanas, que [...] no dispongan [...] [del GEEC], o no estén en disposición de implementarla, o que no dispongan de una herramienta de tramitación electrónica de contratos integrable con los sistemas corporativos de contratación electrónica»; estas entidades tienen la obligación de «tramitar la totalidad de los expedientes y procesos vinculados a la contratación pública, incluidos los menores, mediante el [...] [TEEC], con independencia de los procedimientos, formas e instrumentos utilizados para su adjudicación»; y

   ii. por otra parte, el art. 2.1 prevé igualmente el uso del TEEC «por parte de las entidades de la Administración local catalana y los entes, organismos o entidades de su sector público y por otros entes, organismos y entidades del sector público de Cataluña»;

c. el art. 3.3 de la orden describe detalladamente las funcionalidades que ofrece el TEEC, de entre las cuales cabe destacar, entre otras:

   i. las funcionalidades para la tramitación de expedientes basadas en la gestión de estados del expediente, que determina la información requerida, la documentación y las validaciones exigidas, con posibilidad de avanzar y retroceder en la tramitación a través de las diversas fases de tramitación —preparación, licitación, adjudicación/formalización y ejecución—; hallamos aquí una diferencia relevante con el GEEC en el cual la tramitación se basa en flujos y no en estados, lo que representa un nivel más alto de automatización; el TEEC incorpora un sistema de avisos; asimismo permite dar de alta nuevos circuitos de tramitación adaptados a las especificidades de cada entidad a partir de los estados y validaciones existentes;

   ii. las funcionalidades de gestión documental y de archivo, con incorporación de firma electrónica de los documentos;

   iii. comunicación de la información al RPC y publicación en la PSCP;

d. finalmente, por lo que respecta a la integración con otras aplicaciones y sistemas, el art. 4 de la orden precisa que está prevista la **integración del TEEC con las aplicaciones corporativas** de la Generalitat de Cataluña siguientes:

   i. los sistemas de control de acceso y de autenticación de usuarios, de firma electrónica, de copia auténtica de documentos, y de archivo de documentos electrónicos;

   ii. el RPC, al que el TEEC comunica la información sobre los contratos;

   iii. la PSCP para la publicación de información;

   iv. el servicio de notificaciones electrónicas eNotum; y

v. «otros servicios corporativos para la integración con otros sistemas de información a medida que se producen nuevas necesidades»;

es significativo el hecho de que el TEEC no se integre con los sistemas de información económico-financiera de las entidades usuarias.

Los datos de uso del TEEC[40] indican una utilización más reducida que el GEEC, en términos de usuarios y volumen de tramitación: mientras que en el 2019 se contaban 98 entidades usuarias, en el 2020 eran 97 y en septiembre de 2021 son 96 órganos de contratación con 401 usuarios.

Y por lo que se refiere a sistemas automatizados de alerta de irregularidades, fraude o corrupción en la contratación pública, no consta que la Generalitat de Cataluña ni ninguno de sus organismos disponga de este tipo de sistemas. La referencia del art. 3.2 de la Orden VEH/159/2020, de aprobación del GEEC 2.0 a «alertas y avisos sobre el proceso de tramitación» se tiene que entender en el mismo sentido que la referencia del art. 3.3 de la Orden VEH/159/2020, de aprobación del TEEC, a «un sistema de avisos que permite informar de la fecha límite de presentación de ofertas, la fecha de reuniones de las mesas, la fecha de devoluciones de garantías, etc.».

Debemos señalar, sin embargo, que en el seminario web celebrado el 10/03/2021 titulado *Medios electrónicos e inteligencia artificial al servicio de la integridad en la Contratación pública*[41], la subdirectora general de Regulación y Supervisión de la Contratación Pública manifestó que el desarrollo de este tipo de sistemas de alerta era el siguiente paso en el cual se estaba trabajando.

2.3.2 Ámbito local

A fin de conocer la situación en el ámbito local se ha llevado a cabo una encuesta entre los entes locales que cabe suponer disponen de más recursos y, por lo tanto, en los cuales cabe presumir que la digitalización de la actividad —cuanto menos la de contratación pública— está más desarrollada. A estos efectos se dirigió un cuestionario a un total de 35 entes locales:

a. los ayuntamientos de poblaciones de Cataluña con una población de más de 40.000[42] habitantes;

b. las cuatro Diputaciones provinciales de Barcelona, Tarragona, Girona y Lleida; y

c. el Área Metropolitana de Barcelona.

Las preguntas del cuestionario incidían en los aspectos siguientes:

[40] Datos actualizados a septiembre de 2020. Cfr. nota anterior.

[41] Este seminario puede verse en: https://www.youtube.com/watch?v=wDz9MT_AeeA&t=215s.

[42] Se trata de los ayuntamientos de Barcelona, L'Hospitalet de Llobregat, Terrassa, Badalona, Sabadell, Lleida, Tarragona, Mataró, Santa Coloma de Gramenet, Reus, Girona, Sant Cugat de Vallès, Cornellà de Llobregat, Sant Boi de Llobregat, Rubí, Manresa, Vilanova i la Geltrú, Castelldefels, Viladecans, El Prat de Llobregat, Granollers, Cerdanyola del Vallès, Mollet del Vallès, Vic, Figueres, Esplugues de Llobregat, Gavà, Sant Feliu de Llobregat, Igualada y Vilafranca del Penedès.

a. la solución informática de gestión contable de la entidad y, en el caso que tuviera, la —o las— de tramitación electrónica de expedientes administrativos, distinguiendo entre soluciones parciales —únicamente para determinados trámites del procedimiento: registro, notificaciones, acuerdos y resoluciones, etc.— y soluciones integradas que soportan la tramitación completa del procedimiento, así como los ámbitos materiales en los cuales se utiliza la tramitación electrónica —contratación, ayudas y subvenciones, autorizaciones y licencias, etc.—;

b. la solución informática de tramitación electrónica de expedientes de contratación, en el caso que tuviera, distinguiendo de nuevo entre soluciones parciales y soluciones integradas, y preguntando igualmente si el gestor de expedientes de contratación está integrado con el sistema de información contable (SIC);

c. si el ente dispone de un sistema automatizado de alerta en el ámbito de la contratación pública y, en caso afirmativo, cuáles son las alertas concretas que detecta, indicando algunas posibles [43]; y, en caso negativo, si el ente tiene establecidos mecanismos no automatizados de fiscalización y control interno equivalentes a un sistema de alerta y, en este caso, cuáles de las posibles alertas se detectan por esta vía [43].

Con un 57,14% de respuestas —20 sobre 35 cuestionarios enviados—, los resultados han sido los siguientes:

a. solución informática de tramitación electrónica de expedientes administrativos / parcial o integrada:

Expediente electrónico	Número	Porcentaje
Inexistente	0	0%
Integral	15	75%
Parcial	5	25%
Total	20	100%

[43] Las posibles alertas —automatizadas o no— indicadas en el cuestionario se referían a:

a. fraccionamiento;

b. inadecuación del procedimiento por razón de la cuantía / de las características del contrato;

c. irregularidades en la configuración de la licitación (plazos de presentación de ofertas; exigencias de solvencia; criterios de evaluación; etc.);

d. riesgo / indicios de vínculos entre diversos licitadores;

e. riesgo / incumplimientos de solvencia de licitadores / prohibiciones de contratar;

f. anomalías en las ofertas presentadas (oferta única; número inesperadamente / anormalmente bajo de ofertas; número inusual de ofertas inadmisibles; etc.);

g. detección de ofertas anormalmente bajas;

h. riesgos para la competencia por participación en la licitación de empresas o entidades que han participado en consultas preliminares de mercado;

i. otras (especificar).

b. ámbitos materiales de aplicación de la solución informática de tramitación electrónica de expedientes administrativos —contratación, ayudas y subvenciones, licencias, etc.—:

Ámbitos expediente electrónico	Número	Porcentaje
Contratación	20	100%
Subvenciones	19	95%
Autorizaciones	15	75%
Otros	7	35%
Todos los expedientes	9	45%

c. solución informática de tramitación electrónica de expedientes de contratación / parcial o integrada / integrada con SIC:

Contratación electrónica	Número	Porcentaje
Inexistente	0	0%
Integral	15	75%
Parcial	5	25%
Integrada con el SIC	4	20%

d. sistemas automatizados de alerta:

Sistema automatizado de alerta	Número	Porcentaje
Inexistente	16	80%
Fraccionamiento	2	10%
Inadecuación de procedimiento	1	5%
Irregularidades licitación	1	5%
Colusión / vínculos entre licitadores	1	5%
Solvencia / requisitos para contratar	1	5%
Anomalías ofertas	1	5%
Ofertas anormalmente bajas	2	10%
Riesgos para la competencia	0	0%
Otros	2	10%

e. sistemas no automatizados de alerta:

Sistema no automatizado de alerta	Número	Porcentaje
Inexistente	3	15%
Fraccionamiento	14	70%
Inadecuación de procedimiento	17	85%

Irregularidades licitación	13	65%
Colusión / vínculos entre licitadores	7	35%
Solvencia / requisitos para contratar	10	50%
Anomalías ofertas	11	55%
Ofertas anormalmente bajas	15	75%
Riesgos para la competencia	7	35%
Otros	4	20%

Estos resultados, más que una imagen fiel, deben tomarse como una simple aproximación a la situación real. Efectivamente, cabe razonablemente conjeturar que el grado de digitalización de la parte de las entidades que no han contestado el cuestionario —que representan el 42,86% de la muestra seleccionada— es significativamente más bajo: en este sentido resulta revelador que todas las entidades que han contestado manifiesten que disponen de algún tipo de solución informática de tramitación electrónica de expedientes administrativos.

No obstante, de estos datos podemos extraer un par de conclusiones tendenciales:

a. por una parte, se puede afirmar que la contratación electrónica está lo bastante generalizada en el ámbito local [44];

b. sin embargo, por otra parte, **la implementación de sistemas automatizados de alerta es absolutamente excepcional**, aunque la mayoría de entidades tienen establecidos, a través de los mecanismos fiscalización y control interno, sistemas no automatizados equivalentes a sistemas de alerta.

2.3.3 Perspectivas

Este es pues el panorama: la datificación de la contratación pública es una realidad bastante extendida, pero sólo de forma ultraminoritaria se saca provecho de la misma al servicio de la integridad, implementando sistemas automatizados de alerta basados en datos.

[44] En la versión de 2021 de la *Guia per a la contractació electrònica dels ens locals* (Guía para la contratación electrónica de los entes locales), elaborada y publicada por el Consorcio Localret y accesible en: https://www.localret.cat/guia/nova-versio-2021-de-la-guia-per-a-la-contractacio-electronica-dels-ens-locals/, se indica, con base en datos del Consorcio AOC, que «En 2020 un total de 884 entes locales (de los cuales, 608 ayuntamientos) llevaron a cabo "licitación electrónica" (utilizaron alguna herramienta de licitación electrónica):

- 855 entes locales (601 ayuntamientos) hicieron uso de las herramientas integradas con la PSCP: las herramientas de Sobre Digital y de Presentación Telemática de Ofertas.
- 75 entes locales (33 ayuntamientos) hicieron uso de herramientas de licitación electrónica de operadores privados.

El año 2020, el 85% de las licitaciones abiertas de los entes locales y de las universidades fueron electrónicas».

En este contexto, hay que destacar una iniciativa en curso del Consorcio Localret que abre unas perspectivas prometedoras en el ámbito local. Se trata de una consulta preliminar de mercado, realizada de acuerdo y al amparo de lo que prevé el arte. 115 de la LCSP, para la preparación de la futura licitación de un contrato para dotar los entes locales de **una herramienta de seguimiento, control y planificación de la contratación**.

La consulta fue publicada al perfil de contratante del Consorcio Localret el 17/05/2021 y el informe sobre su resultado fue publicado el 12/07/2021[45].

El informe inicial, justificativo de la conveniencia de llevar a cabo esta consulta de mercado, empieza exponiendo que la misma pretende dar continuidad a la presentación, en febrero de 2020, de la *Guía para la contratación electrónica de los entes locales*, elaborada por el Consorcio Localret con la colaboración de numerosas instituciones de la Generalitat de Cataluña y del ámbito local[46], que tenía «el objetivo principal de delimitar y concretar las principales cuestiones que hacen referencia a la utilización de los medios electrónicos en la tramitación de los procedimientos de contratación, incluyendo propuestas y/o recomendaciones de actuación dirigidas a los órganos de contratación»

El informe destaca acertadamente, en la línea de cuanto se ha venido exponiendo en el presente estudio, que:

> *«**La actividad contractual de las administraciones públicas genera un enorme volumen de datos, que son públicos** —Todos los datos relativos a la actividad contractual están publicados, al menos, en el perfil de contratante y en el Registro Público de Contratos (RPC)—, **pero que**, con carácter general,* [las administraciones públicas] ***no pueden explotar**, o las explotan con hojas Excel y/o con listados poco ágiles. **Los medios electrónicos, informáticos o telemáticos son necesarios para procesar (o estructurar) y analizar estos datos**: las administraciones públicas necesitan una herramienta (informática) que les permita estructurar estos datos, con el fin de poder extraer fácilmente la información necesaria para el seguimiento, control y planificación de la contratación».*

Delimitando el objeto de la consulta, que se concreta en «conocer si hay soluciones disponibles en el mercado que satisfagan las necesidades de los entes locales de seguimiento, control y planificación de su contratación, y, si es el caso, preparar correctamente la licitación de un contrato para dotarnos de esta solución,» el informe especifica que:

> *«Una herramienta (o plataforma) informática de seguimiento, control o supervisión de la ejecución y de planificación de los contratos tendría que tener, al menos, las siguientes funcionalidades:*

[45] Tota la información y documentación sobre esta consulta preliminar de mercado se halla accesible en el perfil de contratante del Consorcio Localret, en: https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/notice.pscp?reqCode=viewCtn&idDoc=93133470.

[46] Cfr. nota 44 anterior.

a) Cuadro de mando que refleje toda la actividad contractual, que permita, por ejemplo, hacer con la antelación suficiente el aviso de prórroga, o anticipar, si es el caso, la preparación de los nuevos contratos.

b) Espacios donde las empresas contratistas puedan depositar la información necesaria para verificar el cumplimiento de los contratos; por ejemplo, de las cláusulas medioambientales, sociales, etc.

c) Espacio de recepción de la prestación, de liquidación del contrato y de gestión de las garantías (ampliación, devolución…).

d) Repositorio documental de pliegos, cláusulas, modelos…»

La consulta se instrumentó mediante un cuestionario publicado en el perfil de contratante del Consorcio Localret que todos los operadores económicos interesados podían completar y presentar. Las preguntas del cuestionario relativas a las funcionalidades de las diversas soluciones hacían referencia los siguientes aspectos:

Funcionalitats	Sí	No
Quadre de comandament dels contractes vigents		
Alertes automatitzades de finalització dels contractes mitjançant l'enviament de correu electrònic		
Alertes predefinides		
Càlcul automatitzat de terminis de tramitació dels expedients de contractació		
Espai on les empreses contractistes puguin dipositar documentació relativa al compliment de les seves obligacions (incloses les obligacions mediambientals i socials).		
Control de l'execució material i pressupostària del contracte: certificacions parcials, actes de recepció, factures, certificació final, vinculació amb les factures, control de la despesa...		
Espai de recepció de la prestació, de liquidació del contracte i de gestió de les garanties (ampliació, retorn...).		
Repositori documental de plecs, clàusules, models...		
Funcions col·laboratives		

[47]

Las dos funcionalidades más interesantes a los efectos del presente informe, evidentemente, son las relativas a «alertas automatizadas de finalización de los

[47] Traducido del catalán:

- Cuadro de mando de los contratos vigentes
- Alertas automatizadas de finalización de los contratos mediante el envío de correo electrónico
- Alertas predefinidas
- Cálculo automatizado de plazos de tramitación de los expedientes de contratación
- Espacio donde las empresas contratistas puedas depositar documentación relativa al cumplimiento de sus obligaciones (incluidas las obligaciones medioambientales y sociales)
- Control de la ejecución material y presupuestaria del contrato: certificaciones parciales, actas de recepción, facturas, certificación final, vinculación con facturas, control del gasto…
- Espacio de recepción de la prestación, de liquidación del contrato y de gestión de las garantías (ampliación, devolución…).
- Repositorio documental de pliegos, cláusulas, modelos
- Funciones colaborativas

contratos» —la continuidad, muy a menudo ilegal, de situaciones contractuales ya finalizadas es una irregularidad bastante frecuente, especialmente en el ámbito local, que, adicionalmente, presenta riesgos relevantes de fraude y corrupción— y «alertas predefinidas». Esta última funcionalidad no quedaba suficientemente concretada en la documentación disponible en el perfil de contratante, si bien en la presentación que se hizo en el Congreso Gobierno Digital [48] se distinguía entre avisos automatizados de finalización de los contratos y *alertas* referidas a fraccionamiento o a la celebración de los mismos contratos con carácter repetitivo.

El otro bloque de preguntas del cuestionario que presenta un gran interés a los efectos que aquí nos interesan es el referido a la obtención de los datos de contratación:

Dades	Sí	No
La solució obté les dades relatives a l'activitat contractual de manera automatitzada*		
La solució permet la introducció i/o correcció manual de dades?		

*D'on obté les dades la solució?
...

[49]

El informe sobre los resultados de la consulta recoge los aspectos más relevantes de las respuestas de las 5 empresas y entidades que participaron, destacando en primer lugar que:

> *«Las empresas […][participantes] tienen una solución de seguimiento, control y planificación de los contratos. En algunos casos, disponen de una solución específica; en otros, es un módulo de una solución más genérica de contratación electrónica (que incluye el tramitador o gestor de expedientes y/o la herramienta de licitación electrónica, etc.). En este segundo caso, […], se trataría de un módulo autónomo […], que, […], los ayuntamientos podrían contratar, sin necesidad de haber de adquirir toda la solución completa…».*

Las diversas soluciones ofrecen la mayoría de las funcionalidades requeridas, si bien se detectan carencias en aquellas relativas a la fase de ejecución, recepción y liquidación de los contratos, y, en lo relativo específicamente a la obtención de datos, el informe indica lo siguiente:

> *«Las **soluciones específicas** de seguimiento, control y planificación de los contratos; es decir, aquellas que no se incluyen dentro de una herramienta o solución más genérica de contratación electrónica,*

[48] En mesa redonda titulada *Minimizando los riesgos en la contratación pública*, que tuvo lugar, en el marco del Congreso Gobierno Digital 2021, el 11/11/2021, el jefe del Área de Contratación del Consorcio Localret presentó esta consulta y sus resultados. Esta mesa redonda puede verse en: https://www.youtube.com/watch?v=xCRzrzin24c&list=PLZSCe8AeXET1wLnwFxPIBTDtmG84vUyVj&index=57&t=1466s

[49] Traducido del catalán:

- La solución obtiene los datos relativos a la actividad contractual de manera automatizada*
- La solución permite la introducción y/o corrección manual de datos?
- * De dónde obtiene los datos la solución?

> ***obtienen los datos*** *(de los contratos)* ***desde las plataformas públicas de contratación****: PLACE y/o PSCP. En principio las* ***soluciones integradas en una solución genérica*** *de contratación electrónica* ***obtienen esta información directamente del tramitador de expedientes o de la herramienta de licitación electrónica propios****, pero advierten que, en caso de que sólo se adquiriera el módulo (autónomo) de seguimiento, esta información se podría obtener de las plataformas públicas de contratación (PLACE y/o PSCP) o también del Registro Público de Contratos (RPC), o, si se requiriera, del propio gestor de expedientes que tenga el ayuntamiento».*

Esta distinción es especialmente importante desde la perspectiva de la disyuntiva entre sistemas de alerta de carácter interno o de carácter externo, que se abordará más adelante.

Finalmente, hay que indicar que el 16/12/2021, el Consorcio Localret inició el procedimiento para la conclusión de un acuerdo marco para la adquisición de una solución informática para el seguimiento, control y planificación de los contratos públicos, con base en los resultados de la mencionada consulta preliminar de mercado [50].

En el apartado 4.° del pliego de prescripciones técnicas, donde se definen las funciones de la solución tecnológica objeto de contratación, se enumeran, entre las «Otras funcionalidades, que inicialmente no se establecen como requisitos mínimos», la de «**Alertas predefinidas de riesgos contra la integridad** de la contratación pública: detección / prevención de irregularidades: fraccionamientos, celebración de los mismos contratos con carácter repetitivo...».

Aunque sería deseable que esta funcionalidad no tuviera carácter optativo, no podemos dejar de saludar la incorporación de esta previsión entre los elementos que configuran el futuro diseño de esta herramienta.

Nota de actualización (septiembre 2022): el procedimiento de licitación para la conclusión del acuerdo marco tramitado por Localret fue resuelto mediante decreto de 15/07/2022. No podemos dejar de señalar que el informe técnico de valoración de las ofertas de acuerdo con criterios cuya cuantificación depende de un juicio de valor, de 20/06/2022, afirma, aunque de forma muy sucinta, que todas las ofertas presentadas incorporaban la mencionada funcionalidad adicional [50]. Que todas las ofertas incorporen alertas de riesgos contra la integridad no deja de ser significativo.

[50] Toda la información y documentación sobre esta licitación se halla accesible en el perfil de contratante del Consorcio Localret: https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/notice.pscp?reqCode=viewCn&idDoc=93360636

3 Referentes

Son numerosísimos los proyectos y las realizaciones que se han desarrollado los últimos años de sistemas basados en el análisis de datos para la detección y prevención de irregularidades, fraude y corrupción en el ámbito de la contratación pública. No tendría sentido intentar hacer una enumeración —necesariamente incompleta— ni mucho menos una descripción exhaustiva de los mismos.

Pero sí que será útil hacer brevemente referencia y describir sucintamente algunos aspectos clave de tres referentes que, a nuestro entender, presentan especial interés: la herramienta Arachne de la Comisión Europea; el sistema SALER de la Comunidad Valenciana; y el documento *Red Flags for Integrity*, publicado por Open Contracting Partnership (OCP).

¿Por qué concretamente estos tres referentes?

a. En cuanto a la herramienta Arachne, porque es la solución tecnológica basada en datos de referencia de la Comisión Europea, considerada por ésta una buena herramienta de lucha antifraude; su importancia como solución ya existente, a la cual se puede adherir toda administración gestora o beneficiaria de los fondos NextGenerationEU, es pues evidente.

b. El sistema SALER de la Comunidad Valenciana fue pionero en el ámbito que aquí nos ocupa, y el marco legal en el cual se fundamenta y que le da cobertura normativa resulta de gran interés.

c. Finalmente, el documento *Red Flags for Integrity* de OCP se puede considerar una referencia inexcusable que no sólo ofrece valiosas orientaciones metodológicas tanto para la implantación como para los diseños de sistemas de alerta basados en datos, sino que igualmente incluye un anexo que, en su última versión, actualizada a mayo de 2021, ofrece un listado detallado de 73 posibles alertas definidas con base en el estándar de datos de contratación pública OCDS diseñado por OCP.

3.1 Herramienta Arachne

Como ya hemos apuntado [51], Arachne es una **herramienta tecnológica integrada de minería y enriquecimiento de datos**, desarrollada por la Comisión Europea desde 2009 y plenamente operacional desde septiembre de 2015, y **puesta**

[51] Cfr. nota 4 anterior. Puede hallarse amplia información sobre la herramienta Arachne en la web oficial de la Comisión Europea: https://ec.europa.eu/social/main.jsp?catId=325&intPageId=3587&langId=es#navItem-relatedLinks, que contiene enlaces a diversos documentos de gran interés, especialmente la presentación y el documento de preguntes frecuentes (únicamente disponibles en inglés), accesibles, respectivamente, en: https://ec.europa.eu/social/main.jsp?catId=738&langId=en&pubId=7883&type=2&furtherPubs=yes (presentación), y en: https://ec.europa.eu/social/BlobServlet?docId=15097&langId=en (preguntas frecuentes).

gratuitamente a disposición de los Estados miembros de la UE[52] con el fin de dar apoyo a las autoridades de gestión y de control de los fondos europeos en su actividad administrativa y de control para **prevenir y detectar errores e irregularidades en los proyectos, beneficiarios, contratos y contratantes**.

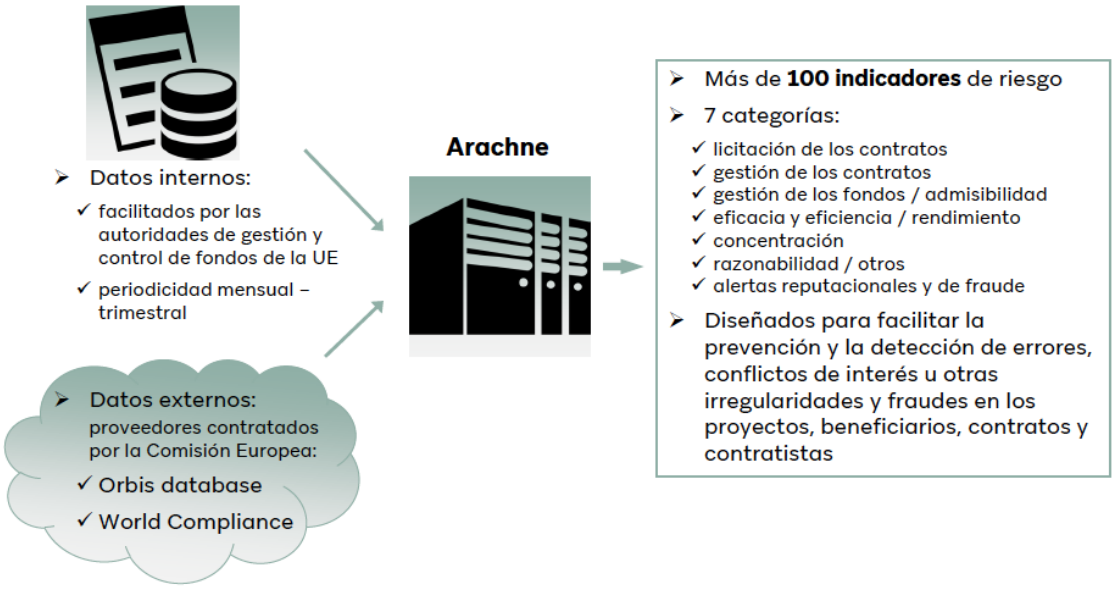
Recordemos en efecto[53] que el art. 125.4 c) del Reglamento (UE) 1303/2013, del Parlamento Europeo y del Consejo, de 17 de diciembre de 2013, sobre disposiciones comunes relativas a los fondos europeos, establece la obligación de «aplicar medidas antifraude eficaces y proporcionadas, teniendo en cuenta los riesgos detectados» en la gestión de aquellos fondos; pues bien, en relación con el cumplimiento de esta obligación la utilización de Arachne, como medida antifraude basada en datos, es considerada el referente por la Comisión[54].

El funcionamiento de la herramienta Arachne es el siguiente: a partir de datos internos, facilitados por los propios entes gestores y de control de los fondos europeos, enriquecidos con datos externos, facilitados por dos proveedores externos, el sistema ofrece hasta 106 indicadores clasificados en 7 categorías: licitación y adjudicación de los contratos, gestión de los contratos, gestión de los fondos (admisibilidad de gastos), rendimiento (eficacia y eficiencia en el uso de los fondos), concentración, razonabilidad y alertas reputacionales y de fraude. Esquemáticamente este funcionamiento se podría representar de la siguiente manera:

[52] La *Carta para la introducción y aplicación de la herramienta Arachne de evaluación del riesgo en las verificaciones de la gestión*, accesible en: https://ec.europa.eu/social/BlobServlet?docId=14836&langId=es, establece un conjunto de principios comunes que tanto las autoridades de gestión de fondos europeos como los servicios de la Comisión se han de comprometer a respectar para la adopción, aplicación e integración de la herramienta Arachne de evaluación de riesgos en los procedimientos de verificación de la gestión de los fondos.

[53] Cfr. nota 34 anterior.

[54] En el documento de preguntas frecuentes se especifica que «Arachne no es de uso obligatorio y por tanto es opcional. Las autoridades de gestión han de implementar medidas antifraude efectivas y proporcionadas de acuerdo con el artículo 125 (4) (c) del Reglamento (EC) 1303/2013 y Arachne puede representar un elemento complementario de estas medidas. Arachne es considerada una buena práctica por la Comisión».



Repasemos brevemente cada uno de los diferentes elementos que integran este sistema.

3.1.1 Datos internos

El art. 72 d) del Reglamento (UE) 1303/2013 impone a los beneficiarios y gestores de fondo europeos la obligación de «contar con sistemas informáticos para la contabilidad, para el almacenaje y la transmisión de los datos financieros y los datos sobre indicadores y para el seguimiento y la elaboración de informes». Estos sistemas informáticos son la fuente de los **datos internos** que utiliza la herramienta Arachne.

En efecto, las organizaciones y entidades usuarias tienen la obligación de transmitir regularmente —idealmente con periodicidad mensual y, como mínimo, trimestralmente; el incumplimiento de esta obligación puede comportar la retirada del acceso a la herramienta Arachne—, en formato XML, extrayéndolas de sus propios sistemas informáticos y cargándolas en un servidor específico de la Comisión Europea, los referidos datos internos para la gestión de los fondos [55]: proyectos, beneficiarios, contratos, contratistas y gastos.

Todos estos datos internos se conservan en el sistema Arachne durante un tiempo limitado, determinado por la normativa sobre gestión de fondos europeos —hasta un máximo de 3 años después de la aprobación por la Comisión de las cuentas anuales de cada programa operativo para la programación 2014-2020—.

[55] Los datos mínimos a transmitir son los especificados en el anexo III del Reglamento delegado (UE) 480/2014 de la Comisión, de 3 de marzo de 2014, que desarrolla el Reglamento (UE) 1303/2013. No obstante, con estos datos mínimos, Arachne no puede calcular todos los indicadores posibles. Las autoridades beneficiarias y gestoras de los fondos pueden, con carácter voluntario, ampliar el número de campos de datos transmitidos al sistema Arachne, a fin de poder disponer de más información e indicadores generados por Arachne. Por ello la Comisión recomienda incluir en los sistemas informáticos de gestión de los fondos europeos todos los campos de datos susceptibles de ser transmitidos a Arachne para su procesamiento, para poder beneficiarse de todo su potencial.

3.1.2 Datos externos

La herramienta Arachne cruza y enriquece los datos internos con **datos externos** facilitados por dos proveedores externos contratados por la Comisión Europea:

a. Bureau Van Dijk, que facilita la información de su base de datos **Orbis database**, con datos financieros (volumen de negocio, flujo de caja, beneficios, etc.) e información sobre accionistas, filiales, sede social, tipo y magnitud de la empresa, sector de actividad, representantes oficiales y otros indicadores de credibilidad y solvencia de más de 200 millones de empresas de todo el mundo; y

b. LexisNexis, que aporta la base de datos **World Compliance**, con listados de personas políticamente expuestas (PEP) —personas que ocupan cargos públicos especialmente susceptibles de encontrarse con situaciones de conflicto de interés—, personas y entidades sancionadas y vinculadas a actividades delictivas (tráfico de drogas o de personas, blanqueo de capitales, fraude fiscal o financiero, etc.) así como informaciones adversas en los medios de comunicación.

Estos proveedores externos de datos fueron seleccionados por la Comisión Europea [56] después de un estudio de mercado, basándose especialmente en el hecho de que los datos de dos bases de datos mencionadas provenían de fuentes oficiales de acceso público [57] y no de fuentes no oficiales o poco fiables. Adicionalmente es responsabilidad de estos dos proveedores externos garantizar la calidad y la fiabilidad de los datos facilitados.

Los datos externos son actualizados con periodicidad trimestral.

Por último cabe señalar, en relación con el tratamiento por Arachne tanto de los datos internos como de los externos, desde el punto de vista del régimen legal de protección de datos, que la Comisión Europea presentó ante el Supervisor Europeo de Protección de Datos la notificación correspondiente obteniendo un dictamen favorable sobre el cumplimiento por Arachne de las disposiciones del Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre 2000, relativo a la protección de las personas físicas con respecto al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos —actualmente derogado y sustituido por el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, del 23 de octubre de 2018—. Por su parte, las autoridades nacionales usuarias de Arachne deben de cumplir igualmente las normas nacionales y

[56] La Comisión Europea concluyó un contrato marco con una duración que cubría el plazo de finalización de la programación 2014-2020. Está prevista una evaluación del impacto y la utilidad de la herramienta Arachne que determinará, en función de les disponibilidades presupuestarias, la eventual renovación del contrato a fin de continuar garantizando la gratuidad de la utilización de Arachne por las autoridades nacionales.

[57] Los datos sobre sanciones y personas o entidades sancionadas son objeto de tratamiento de conformidad con lo dispuesto en el art. 11 del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unió, y a la libre circulación de esos datos.

europeas en materia de protección de datos, lo que implica, entre otras consecuencias, que los datos e indicadores de riesgos facilitados por Arachne no pueden ser publicados.

3.1.3 Indicadores generados por Arachne

A partir de los datos internos y externos, Arachne genera 106 indicadores clasificados en 7 grandes categorías [58]:

a. contratación pública: 6 indicadores referidos a los procedimientos de licitación y adjudicación de los contratos financiados con fondos europeos;

b. gestión de los contratos: 10 indicadores relativos a la gestión de la ejecución de los contratos en función de los datos comparativos con contratos de características análogas;

c. admisibilidad de gastos: 14 indicadores para la gestión de los fondos, que permiten verificar la admisibilidad de los gastos a financiar tanto desde el punto de vista temporal como material;

d. rendimiento: 18 indicadores de eficacia y eficiencia en la utilización de los fondos, que permiten evaluar la coherencia de la actividad subvencionada en función de los referentes sectoriales;

e. concentración: 13 indicadores diseñados para facilitar la detección de concentraciones de fondos europeos en los mismos beneficiarios, mediante el cruce de datos a nivel de proyectos y programas;

f. otros: 16 indicadores básicos sobre coherencia y razonabilidad de los proyectos; y

g. alertas reputacionales y de fraude: 30 indicadores que cubren los 5 ámbitos de riesgo siguientes:

    i. riesgos financieros: 6 indicadores de la situación financiera de los beneficiarios y participantes en los proyectos, contratistas y subcontratistas e integrantes de uniones de empresas, basados en datos financieros;

    ii. riesgos de vinculaciones: 7 indicadores referidos la existencia de posibles vinculaciones entre los beneficiarios y participantes en los proyectos, contratistas y subcontratistas e integrantes de uniones de empresas;

    iii. riesgos reputacionales: 6 indicadores sobre participación en actividades que puedan comportar un perjuicio reputacional;

    iv. sanciones: 4 indicadores de la aparición de los beneficiarios y participantes en los proyectos, contratistas y subcontratistas e integrantes de uniones de empresas en cualquier tipo de listas de entidades sancionadas o en situación de prohibición de contratar;

    v. cambios: 6 indicadores de cambios en la estructura de las empresas o entidades.

[58] Esta descripción se basa en el documento de la Comisión Europea *Arachne. What is new in Arachne v2.0*, de 16/02/2017, accesible en el enlace indicado en la nota 51 anterior.

Cabe precisar que un valor alto de riesgo indicado en un indicador concreto no se puede considerar de ninguna manera una prueba de la existencia de una irregularidad de cualquier tipo. En este sentido, Arachne debe considerarse un sistema de a*lerta*, que, mediante la información que genera, indica la *posible o potencial* existencia de alguna irregularidad, lo que —la menos en teoría— debería dar lugar a la correspondiente verificación o investigación para confirmar o descartar su existencia efectiva.

Resulta especialmente interesante que Arachne permita igualmente a las autoridades nacionales introducir en el sistema los datos de las personas integrantes de las mismas que estén involucradas en la gestión y control de los fondos europeos, siempre, evidentemente, dentro del respeto de las disposiciones nacionales y europeas en materia de protección de datos.

Los indicadores generados por Arachne facilitan información, en términos de niveles de riesgo, referida a los diversos beneficiarios, contratistas y subcontratistas, útil en las diversas fases de la gestión de los fondos. Así:

a. en las fases de selección de los beneficiarios y adjudicación de los contratos los indicadores permiten detectar los riesgos vinculados a situaciones de conflicto de interés, de incumplimiento de las normas europeas sobre ayudas de estado o de falta de capacidad administrativa o de solvencia, entre otros;

b. en las fases de ejecución de los proyectos los indicador facilitan alertas sobre riesgos de errores o irregularidades en la contratación y ejecución de contratos, admisibilidad de gastos, concentración de fondo en los mismos beneficiarios, bajos rendimientos o inconsistencias en los proyectos; y

c. en la fase final de auditoría y evaluación de los proyectos concluidos, los indicadores permiten evaluar los impactos positivos de los mismos.

No obstante, hay que puntualizar igualmente que los indicadores de Arachne también presentan algunas limitaciones. Así, por ejemplo, no permiten detectar situaciones de colusión entre licitadores, ni la acumulación en un mismo beneficiario de fondos europeos y de otros tipos de subvenciones incompatibles. Y, con respecto a la detección de los conflictos de interés, Arachne sólo puede detectar vinculaciones de naturaleza jurídica, correspondiente al hecho de ocupar formalmente cargos o puestos en las diversas entidades analizadas; la existencia de lo que se podría denominar **vinculaciones privadas o difusas** —relaciones de negocios, familiares, de amistad, u otras análogas— no son susceptibles de ser detectadas por la herramienta Arachne. Esta es una limitación que el sistema SALER aspira a superar.

3.2 Sistema SALER

El sistema SALER es un proyecto pionero de la Generalitat Valenciana cuya implementación operativa se encuentra en desarrollo constante y de que resulta de gran interés el **diseño a nivel normativo**, establecido en la Ley 22/2018, de 6 de noviembre, de la Generalitat, de Inspección General de Servicios y del sistema de alertas para la prevención de malas prácticas en la Administración de la Generalitat y su sector público instrumental.

De hecho, es el primer intento de aplicar el planteamiento que defendemos en este estudio: **sacar provecho de la datificación de la actividad del sector público al servicio de la integridad**, implementando sistemas automatizados de alerta basados en datos. Así lo explicita la exposición de motivos de la Ley 22/2018 que afirma las siguientes premisas sobre las cuales se fundamenta el diseño del sistema:

> *«La sofisticación cada vez mayor de los procesos de obtención, almacenamiento y análisis de datos representa una importante oportunidad para la prevención de irregularidades y malas prácticas. […] resulta factible* ***aprovechar las posibilidades que ofrece el análisis de datos para enriquecer de forma significativa el proceso de evaluación del riesgo****. Así,* ***mediante la utilización e interconexión de los datos con los que cuenta la administración pública resulta posible detectar probables situaciones de riesgo, incluso antes de que se acaben produciendo irregularidades****. […]*
>
> *… esta ley garantiza el correcto manejo de una herramienta de prospección de datos, el sistema de alertas rápidas, para identificar los procesos administrativos que pueden ser susceptibles de presentar riesgo de irregularidades o malas prácticas. Este sistema es un instrumento de clasificación e identificación del riesgo que va dirigido a reforzar la identificación, prevención y detección temprana de estas prácticas en los procesos administrativos de gestión. […]*
>
> *Este sistema de alertas, junto con la elaboración de un mapa de evaluación de riesgos, los planes individuales de autoevaluación y la publicación de un código de buenas prácticas para la prevención y detección de irregularidades, constituirán los instrumentos básicos de carácter preventivo que permitirán reducir los riesgos de irregularidades o malas prácticas administrativas.»*

Existe poca información o documentación publicada sobre el sistema SALER y por eso resulta de lo más interesante un artículo publicado en octubre de 2019 por Alfonso PUNCEL CHORNET, subsecretario de la Consejería de Transparencia del Gobierno valenciano entre julio de 2015 y julio de 2019 y, como tal, responsable de la Inspección General de Servicios (IGS) y del diseño y desarrollo del sistema SALER, en el que se detallan los antecedentes y las circunstancias de la concepción del sistema, y se describen a nivel general e introductorio sus principales aspectos [59].

En el mencionado artículo se destacan especialmente los retos a los cuales se tuvo que hacer frente en la concepción y el diseño del sistema SALER, el primero de los cuales era, precisamente, la falta de ningún referente preexistente:

[59] Artículo *Inteligencia artificial para la transparencia pública. El Sistema de Alertas Tempranas (SALER) de la Generalitat Valenciana*, publicado en el núm. 3116, de octubre de 2019 del Boletín Económico del ICE, págs. 41 a 61; accesible en: http://www.revistasice.com/index.php/BICE/article/view/6914/6928

> *«… se planteó la posibilidad de disponer de un sistema de alertas de malas prácticas e irregularidades, que se fue puliendo hasta llegar a una primera propuesta, […], aunque* ***tuvimos que crear un modelo completo porque no encontramos ningún sistema que pudiera servir de referente****. Todos los sistemas estudiados se remitían a cuadros de mando o modelos de autoevaluación cualitativa […], siendo el más complejo el ARACHNE, utilizado por la Administración europea para el seguimiento y control de los fondos europeos. Pero aun con todo, no era exactamente lo que queríamos construir, entre otros motivos porque nuestra intención fue siempre alcanzar todos los ámbitos de gestión pública y no solo aquellas áreas relacionadas con la gestión de recursos económicos o presupuestarios.»*

Efectivamente, el sistema SALER no limita su ámbito de aplicación a la contratación pública, sino que aspira a «obtener alertas sobre malas prácticas en diferentes procesos de gestión (contratación, utilización del patrimonio público, selección de personal, incompatibilidades, concesión de ayudas, subvenciones, etc.)»[60]. Otros retos surgieron a la hora de posibilitar el acceso a los datos por parte de la IGS, responsable y gestora del sistema SALER, así como de hacer frente a las dinámicas y resistencias al cambio de la administración[61].

Pero el reto principal fue **transformar el conocimiento administrativo sobre riesgos de posibles malas prácticas e irregularidades en los algoritmos que, a partir de los datos disponibles, generasen las alertas** correspondientes.

En palabras de PUNCEL CHORNET: «… el verdadero "corazón" del proyecto […] está en el conocimiento administrativo y en la parte creativa de definir riesgos, alertas, algoritmos […]. De hecho, la parte más compleja era definir, para cada ámbito de gestión, los indicadores y los patrones de normalidad que nos permitieran disponer de alertas cada vez más precisas y efectivas», es decir: «establecer patrones de comportamiento "normal" y determinar aquellos comportamientos que se salen de dichos patrones predefinidos como normales y que podrían ser indicativos de malas prácticas o irregularidades».

La descripción general del funcionamiento del sistema SALER es, según PUNCEL CHORNET, la siguiente:

> *«La idea del SALER es muy simple. Se trata de utilizar la creciente información digitalizada de la que dispone la Administración de la Generalitat Valenciana y toda aquella información externa (bases de datos de registradores, notarios, entidades de propiedad intelectual, etcétera) que sea relevante para analizar cualquier procedimiento administrativo y que sea de interés para las funciones de un compliance*

[60] Op. cit. pág. 45. Cfr. nota anterior.

[61] Op. cit. pág. 51: «… el problema fue convencer al propietario de la información del buen uso que se iba a hacer de ella, o salvar las reticencias al control de la información»; pág. 53: «… las dificultades tecnológicas no procedieron de la falta de aplicaciones, entorno a utilizar o posibilidades reales existentes en el mercado, sino de la propia dinámica interna de la Generalitat Valenciana y de las estructuras de apoyo tecnológico muy anquilosadas y dedicadas a las tareas más simples de tecnificación de la Administración». Cfr. nota 59 anterior.

officer convertido en información digital (prácticamente cualquier información administrativa puede convertirse, incluso aquella más cualitativa) para ser tratada digitalmente.

A estos datos digitalizados les aplicamos "instrucciones o reglas bien definidas, ordenadas y finitas que permiten llevar a cabo una actividad mediante pasos sucesivos que no generen dudas a quien deba hacer dicha actividad"; es decir, aplicamos algoritmos matemáticos e informáticos para averiguar si estos cumplen con determinadas pautas o se salen de la conducta normal, en cuyo caso activaría una alerta que se convierte en un aviso para que la IGS actúe de la forma más rápida y menos burocrática para identificarla (origen, procedimiento, ámbito de gestión gestor involucrado) y clasificarla (positivo o falso positivo), y, en caso de tratarse de una alerta positiva, resolverla.».

La translación y el desarrollo de esta idea en sede normativa se encuentra en el capítulo I, titulado precisamente *Sistema de alertas*, del título II de la Ley 22/2018, que incluye dos secciones:

a. la primera, *Elementos del sistema de alertas, adscripción e instrumentos de gestión del riesgo* —arts. 17 a 24—, que contiene la definición y descripción de los diversos elementos que integran el sistema de alertas; y

b. la segunda, *Características técnicas y funcionales del sistema* —arts. 25 a 29—, más centrada en aspectos relativos al funcionamiento operativo del sistema: la compatibilidad, desarrollo, explotación y mantenimiento del sistema informático; las garantías de seguridad del sistema; la clasificación de riesgos y codificación de resultados de las actuaciones de investigación de la IGS; el código de buenas prácticas y los protocolos de actuación; y las previsiones de evaluación periódica del sistema.

Así, el art. 17 de la Ley empieza, en su apartado 1.°, describiendo el sistema SALER, indicando que «... se articulará a través de un conjunto de herramientas cuya interacción permite la detección de posibles irregularidades y malas prácticas administrativas, con carácter preventivo, a partir del análisis de la información obtenida y de la evaluación de factores de riesgo que potencialmente pudieran originarlas».

A partir de esta definición general, los siguientes preceptos de la ley describen minuciosamente los diversos **elementos que integran el sistema SALER**, que, de acuerdo con el art. 17.2 de la Ley 22/2018, son los siguientes:

a. los **datos** —art. 17.2 a)—, provenientes tanto de bases de datos propias de la Generalitat valenciana —art. 18 de la Ley— como de otros organismos o entidades —art. 19— e igualmente —y eso es especialmente interesante— obtenidos de fuentes abiertas, particularmente de Internet —art. 17.3; enseguida volveremos con más detalle sobre este aspecto—;

b. el **sistema lógico e informático de procesamiento de datos** —art. 17.2 b)—, constituido, según establece el art. 20 de la Ley, por «El conjunto de herramientas de software y la infraestructura de servidores y bases de datos con que funcionan», «El conjunto de datos obtenidos mediante procesos de extracción, transformación y carga a partir la información

contenida en las bases» y «Los mecanismos de análisis de datos que, a través de indicadores de riesgo definidos para cada uno de los diferentes ámbitos de gestión administrativa sobre los que actuará el sistema, permitan la detección de situaciones irregulares susceptibles de investigación»;

c. las **evaluaciones**, el **mapa de evaluación de riesgos** y las **autoevaluaciones individuales** —art. 17.2 c)—, regulados, respectivamente, en los arts. 21, 22 y 23 de la Ley; y

d. los **informes de conclusiones y recomendaciones** de cada actuación de investigación de la IGS y también los **informes de evaluación del propio sistema** SALER que lo retroalimentan —art. 17.2 d)—.

Como acabamos de ver, los datos que utiliza el sistema no sólo provienen de bases de datos internas de la Generalitat valenciana y de su sector público instrumental, o de otros organismos y entidades, sino también de fuentes abiertas. Este es uno aspectos especialmente interesante del sistema SALER, con el cual aspira a superar alguna de las limitaciones ya apuntadas de la herramienta Arachne.

Esta posibilidad plantea, sin embargo, cuestiones relevantes desde el punto de vista de la protección de datos personales. Y a este respeto la exposición de motivos de la Ley destaca el siguiente:

> *«La puesta en marcha del sistema de alertas […] comporta el **tratamiento de datos personales de personas físicas** que resulten relevantes para el cumplimiento de sus fines, siempre respetando sus derechos, especialmente los fundamentales, […]. Los datos a tratar se circunscriben a las personas que mantengan, o hayan mantenido, cualquier relación jurídica con la administración de la Generalitat, […].*
>
> *Los datos pueden proceder de tres fuentes: bases de datos internas creadas y mantenidas por la administración de la Generalitat y su sector público instrumental con los datos que los interesados han proporcionado voluntariamente para la tramitación del procedimiento a través del cual se han relacionado con la administración; bases de datos de organismos o entidades externas con los que se establezca una colaboración, por ejemplo registros públicos; y, finalmente, **datos de carácter personal que sus titulares hayan hecho manifiestamente públicos**, particularmente en internet.*
>
> *Con respecto al último grupo de datos, debe clarificarse que su tratamiento se limita exclusivamente a aquellos datos que resulten relevantes para el desarrollo de una investigación en la medida en que puedan permitir detectar signos externos de un nivel adquisitivo desproporcionado, relaciones entre los interesados o entre estos y el personal al servicio de la administración pública o su sector público instrumental, por ejemplo.»*

Aun así, la exposición de motivos de la ley afirma la compatibilidad de sus previsiones con las disposición 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 con respecto al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), precisando que el tratamiento de los datos personales llevado a cabo por el sistema SALER se ampara en el art. 6 c) y e) del RGPD —tratamiento para el cumplimiento de una obligación legal y/o para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos—.

Estas cautelas y prevenciones en materia de protección de datos se observan muy claramente en la regulación, en el art. 17.3 de la Ley, relativo a los datos personales obtenidos de fuentes abiertas, que dispone el siguiente:

> *«También se podrán integrar en el sistema datos personales de personas o entidades que tengan o hayan tenido una relación directa con la administración de la Generalitat y su sector público instrumental referidos a expedientes administrativos relacionados con la contratación, con ayudas o subvenciones públicas, así como de las personas o entidades que mantengan o hayan mantenido una relación laboral o contractual con la administración de la Generalitat y su sector público instrumental.*
>
> *Para las finalidades previstas en esta ley podrán tratarse los **datos que los interesados** descritos en el párrafo anterior **hayan hecho manifiestamente públicos de manera voluntaria, particularmente en internet**.*
>
> *Para ello, deberán reunirse las siguientes condiciones:*
>
> *a) Que tales espacios tengan la condición de **abiertos** y **no estén protegidos por el derecho a la intimidad o el derecho al secreto de las comunicaciones**.*
>
> *b) Que, en el caso de redes sociales, se trate de páginas indexables por buscadores, espacios abiertos a todos los miembros de la red, redes sociales abiertas o redes cuya naturaleza profesional, empresarial o similar **permitan excluir toda expectativa de privacidad**.*
>
> *c) Que en ningún caso sean objeto de tratamiento los datos de terceras personas relacionadas con los investigados.»*

Estas previsiones se completan con una **explícita regulación del plazo de conservación de los datos** y de las **limitaciones a los derechos reconocidos por el RGPD**. La exposición de motivos de la Ley precisa que «teniendo en cuenta que el ejercicio de malas prácticas e irregularidades muchas veces solo puede detectarse si se analizan los datos acumulados en un período de tiempo, resulta imprescindible para el cumplimiento de los fines del sistema que la ley, de acuerdo con las posibilidades que ofrece el reglamento europeo, regule dos aspectos fundamentales que tienen incidencia directa sobre esta capacidad de análisis: un plazo amplio de conservación de los datos, que se sitúa en ocho años, y la limitación de los derechos regulados en los artículos 12 a 22 del reglamento».

La Ley 22/2018 entraba en vigor, de acuerdo con su disp. final 2.ª, a los 20 días de su publicación en el DOGV, que tuvo lugar el 08/11/2018, pero el 2.° inciso de la mencionada disp. final 2.ª preveía que las previsiones relativas al sistema SALER entrarían en vigor en el momento en que se determinara por el consejero o consejera responsable de la IGS, dentro de un plazo máximo de 6 meses desde la publicación de la ley. Esta previsión se cumplió mediante resolución de 31/01/2019 del Consejero de Transparencia, Responsabilidad Social, Participación y Cooperación, publicada en el DOGV el 07/02/2019.

Hemos visto que uno de los principales retos en el diseño e implementación del sistema SALER fue precisamente convertir, a partir del conocimiento administrativo sobre posibles riesgos, los datos en alertas, mediante los algoritmos correspondientes. Pues bien, para esta tarea resulta extremadamente útil el estudio *Red Flags for Integrity* publicado por OCP en 2016.

3.3 Documento *Red Flags for Integrity* (OCP, 2016-2021)

Open Contracting Partnership es una colaboración «entre gobiernos, empresas, la sociedad civil y especialistas en tecnología para hacer transparente y transformar la contratación pública en todo el mundo», creada inicialmente por el Banco Mundial y establecida en el 2015 como programa independiente sin ánimo de lucro, patrocinado por el Fund for the City of New York (Fondo para la Ciudad de Nueva York [62].

OCP ha llevado a cabo numerosos proyectos, pero a los efectos de este estudio, dos son de especial interés:

a. el Estándar de Datos de las Contrataciones Abiertas (OCDS, por el acrónimo de la denominación oficial en inglés: *Open Contracting Data Standard*); y

b. el ya mencionado documento *Red Flags for Integrity: Giving the green light to open data solutions* (Banderas rojas para la integridad: luz verde a las soluciones basadas en datos abiertos), publicado por OCP en 2016.

El OCDS es un estándar de datos abiertos de contratación pública que «permite la divulgación de datos y documentos en todas las etapas del proceso de contratación mediante un modelo de datos común» y fue creado «para ayudar a las organizaciones a aumentar la transparencia de la contratación y permitir un análisis más profundo de los datos contratación por parte de una amplia gama de usuarios», tal como se indica en la web oficial correspondiente [63].

[62] Información sobre OCP en su página web oficial, accesible en: https://www.open-contracting.org/es/about/

[63] Toda la información disponible sobre el OCDS se encuentra, en inglés (versión oficial de referencia), francés y castellano en la web oficial: https://standard.open-contracting.org/latest/es/

La información disponible en esta web incluye una presentación e introducción general al OCDS, una guía para el diseño e implantación del OCDS en cualquier organización, la definición detallada del modelo de datos y las reglas de aplicación correspondientes, herramientas de ayuda e indicaciones para la obtención de asistencia para la implantación del OCDS, el histórico del

Por su parte, el documento *Red Flags for Integrity* es una publicación de OCP de noviembre de 2016 que consta de dos documentos:

a. el documento *Red Flags for Integrity* propiamente dicho, que constituye una guía metodológica muy práctica para el diseño e implementación de un sistema de alerta en el ámbito de la contratación pública; y

b. el documento complementario *Red Flags to OCDS Mapping*, en formato de hoja de cálculo, que, en su versión más reciente, de mayo de 2021, contiene un listado de 73 posibles alertas —el documento utiliza el término *red flag* (bandera roja), de uso habitual a nivel internacional; utilizaremos la traducción: *alerta*—, detalladamente definidas mayoritariamente a partir de los datos del modelo OCDS; tal como se indica en el propio documento, esta nueva versión del listado es el resultado de depurar el listado originario de 2016 —con 119 posibles alertas— eliminando duplicidades y algunas alertas basadas en datos no incluidos en el modelo OCDS, y de añadir nuevas alertas; asimismo, la nueva versión incluye el detalle de los datos del modelo OCDS necesarios para cada alerta, el método de cálculo aplicado, la descripción y la explicación de la alerta y los documentos de referencia —publicaciones académicas o de investigación— en los cuales se basa cada alerta [64].

No tiene, evidentemente, sentido reproducir aquí el documento en cuestión, pero vale la pena remarcar especialmente algunas reflexiones y consideraciones metodológicas, especialmente acertadas y útiles, contenidas en lo mismo.

3.3.1 Interés y utilidad de los sistemas de alerta

La primera idea en la que incide el documento es el **enorme potencial de los sistemas de alerta basados en el análisis de datos en tiempo real**, en la medida en que permiten detectar las posibles irregularidades y los riesgos potenciales de fraude y corrupción antes de que se haya consumado su producción y se hayan verificado los riesgos [65].

En este sentido, el documento destaca especialmente cómo se constata una evolución en los estudios sobre corrupción desde una perspectiva reactiva y punitiva hacia nuevas aproximaciones centradas en el control de la

estándar OCDS y una herramienta de revisión de datos para la verificación de la correcta implantación de este modelo de datos abiertos de contratación pública.

[64] Tanto el documento *Red Flags for Integrity* como el documento complementario *Red Flags to OCDS Mapping* se encuentran en página oficial de OCP, accesibles, lamentablemente **sólo en inglés**, en: https://www.open-contracting.org/es/resources/red-flags-integrity-giving-green-light-open-data-solutions/

Puede hallarse más información sobre el documento, sus objetivos y los expertos que participaron en su elaboración, entre otros, en la publicación de 30/11/2016 del blog de OCP accesible en: https://www.open-contracting.org/es/2016/11/30/red-flags-integrity-giving-green-light-open-data-solutions/

[65] *Op. cit.* pág. 4: «Una de las promesas más interesantes del análisis de datos en tiempo real en contratación pública es que la corrupción y el fraude pueden potencialmente ser detectados y prevenidos antes de ocurrir, en lugar de dejar que los poderes públicos arreglen los destrozos *a posteriori*».

contratación mediante **sistemas de alerta**, insistiendo en su **carácter intrínsecamente proactivo**[66], y destacando como estos sistemas se alinean con los planteamientos del documento *Principios de datos abiertos anticorrupción* aprobado por el G20 y de la *Carta internacional de Datos Abiertos*, a los cuales ya nos hemos referido[67].

Asimismo, el documento incide en una idea ya apuntada —al tratar la herramienta Arachne; cfr. apartado 3.1.3 anterior—: que, en general, los indicadores de alerta no se tienen que considerar pruebas concluyentes de irregularidades, fraude o corrupción, sino únicamente *indicios* de la existencia de un hecho o una circunstancia anómala, que justifica una revisión o investigación más esmerada.

3.3.2 Ideas clave

Desde una perspectiva conceptual, debemos destacar 3 ideas clave del documento que nos ocupa que, como precisa en su introducción, pretende dar respuesta a dos cuestiones esenciales: qué datos son necesarias para la detección de las irregularidades, el fraude y la corrupción, y cómo pueden utilizarse y porqué.

Primera idea: la **importancia del contexto**. Varios estudios generales demuestran que, con carácter general, las irregularidades y los comportamientos constitutivos de fraude o de corrupción en la contratación pública se pueden reconducir a cuatro grandes categorías o esquemas ilícitos[68]. Eso hace que las diversas alertas sean homologables y aplicables, a nivel conceptual, en varios países y contextos, en la medida en que el esquema ilícito subyacente es lo mismo. No obstante, es absolutamente necesario, a fin de que las alertas concretamente diseñadas operen de forma eficiente y eficaz,

---

[66] *Op. cit.* pág. 6: «Puede ser también más efectivo centrarse en desarrollar planteamientos proactivos más que reactivos para el control de la contratación pública, mediante sistemas de alerta. […] Desde este punto de vista, los sistemas de alerta son una herramienta proactiva, y no meramente reactiva».

[67] Cfr. apartado 2.1.2 anterior (págs. 17 y 18) y notas 16 y 17.

[68] El documento *Red Flags for Integrity* fundamenta esta afirmación principalmente en la *Guía para la lucha contra la corrupción y el fraude en los proyectos de desarrollo* (*Guide to Combating Corruption & Fraud in Development Projects*) —accesible (en inglés) en: https://guide.iacrc.org—, elaborada por el Centro Internacional de Recursos Anticorrupción (International Anti-Corruption Resource Center) —web oficial: https://iacrc.org—, así como en los trabajos en los cuales se basa el proyecto *DIGIWHIST, The Digital Whistleblower* —cfr. nota 2 anterior—.

Las 4 grandes categorías serían las siguientes:

a. la corrupción propiamente dicha, que incluiría el soborno y comisiones y los intereses ocultos;

b. la manipulación de licitaciones, que incluiría diversas tipologías de irregularidades con incidencia en el proceso de licitación —irregularidades en la información sobre la licitación, en la definición de las especificaciones y requisitos, en la selección de los licitadores, en los criterios de adjudicación, en la formación de las ofertas, fraccionamiento, etc.—;

c. la colusión entre licitadores; y

d. el fraude, referido a la fase de ejecución de los contratos, una vez adjudicados, que incluiría también varias tipologías de irregularidades —incumplimientos contractuales, falsa facturación, modificaciones irregulares, etc.—.

contextualizar el diseño general adaptándolo a las singularidades de cada marco legal y contexto social y económico. Esta adaptación al contexto concreto en el cual tiene que operar la alerta es especialmente importante con el fin de evitar falsos positivos: alertas que no corresponden a ninguna irregularidad real ni potencial, provocadas por deficiencias en la definición de los valores umbrales de los datos utilizados que hacen saltar la alerta.

Segunda idea: conveniencia de utilizar una **estrategia de "triangulación",** entendida como la **utilización agregada de más de un dato** como indicador con el fin de obtener alertas más robustas y fiables.

A este respecto, el documento destaca como el uso de valores promedio de un único dato para definir una alerta aumenta el riesgo de generar falsos positivos. Con el fin de evitar este riesgo, una posible estrategia es precisamente definir la alerta combinando varios datos, relativos a diferentes aspectos del fenómeno analizado, con el fin de generar un indicador compuesto más fiable.

Tercera idea: la importancia crucial de la **disponibilidad y calidad de los datos** a utilizar. El diseño de alertas requiere necesariamente disponer de datos en cantidad suficiente —para permitir la comparación y el establecimiento de valores promedio de referencia, que permitan detectar anomalías— y de calidad —los datos tienen que ser fiables y no tienen que contener errores ni carencias significativas—.

El documento destaca especialmente el interés de cruzar y analizar conjuntamente los datos de contratación pública, en sentido estricto, y datos de otros tipos —aunque, evidentemente, relacionados con la contratación— como serían datos mercantiles, financieras, de titularidades reales de empresas, de vinculaciones entre entidades, etc.

Volveremos sobre esta importante cuestión al tratar la tipología de sistemas de alerta en el apartado 4.3 siguiente.

3.3.3 Metodología

El apartado III del documento *Red Flags for Integrity* resulta especialmente interesante a los efectos del presente estudio en la medida en que presenta los **5 pasos metodológicos** seguidos para la creación del listado de posibles alertas del documento complementario [69].

El interés de este pasos metodológicos es tanto más grande en cuanto que son **generalizables y extrapolables a cualquier proceso de diseño e implantación de un sistema de alerta** en cualquier organización. Por eso, a continuación y al hilo de la exposición de aquellos pasos, iremos apuntando en qué términos se

[69] *Op. cit.* pág. 12: «Nuestra aproximación a la detección de la corrupción es simple: hemos compilado alertas de riesgo de corrupción a lo largo del ciclo de contratación, desarrollado indicadores para cada alerta y definido estas alertas mediante cómputos claros y replicables. Hemos definido entonces estos cómputos utilizando los campos de datos del estándar OCDS, permitiendo que cualquiera que disponga de este estándar pueda calcular los indicadores. Los pasos siguientes incluyen poner a prueba los indicadores utilizando diversas fuentes de datos OCDS para evaluar su integridad en los diversos mercados de contratación pública».

podrían adaptar, a nuestro entender, al proceso concreto de diseño e implantación de un sistema de alerta.

Los cinco pasos metodológicos son los siguientes:

Primero: **identificar las posibles alertas**. El primer paso de los autores del documento fue recopilar un listado de alertas, de posibles indicadores de riesgos de irregularidades, fraude o corrupción en los procesos de contratación pública. La perspectiva generalista del documento, y su vocación de referente en el ámbito que nos ocupa determina que la recopilación que hicieron fuera la más amplia y omnicomprensiva posible, intentando establecer cualquier alerta que se considerara «observable, coleccionable y relevante».

Ahora bien, en cualquier organización que aspire a diseñar e implementar un sistema automatizado de alerta este primer paso es igualmente importante, no tanto con el objetivo de listar *todas* las posibles alertas imaginables —para eso ya existe el documento complementario de OCP con el listado de 73 posibles alertas—, sino para establecer **qué alertas concretas son útiles y relevantes teniendo en cuenta las características de la organización**.

Efectivamente, parece evidente que el sistema de alerta adecuado para un ayuntamiento pequeño o de tamaño medio con limitaciones y deficiencias de capacidad de gestión administrativa no será el mismo que el requerido para un gran ente local con una estructura organizativa amplia y de gran capacidad de gestión, o para una entidad gestora de grandes infraestructuras: se puede razonablemente conjeturar que las alertas más relevantes y útiles en el primer caso se centrarán en aspectos procedimentales —fraccionamientos derivados de deficiencias de planificación y gestión; situaciones irregulares de continuidad de prestaciones de contactos ya concluidos, por ejemplo—; en el segundo probablemente tendrán importancia la detección de situaciones de conflicto de interés o irregularidades en la fase de ejecución; y en el tercero será mucho más útil poner el foco en posibles riesgos de colusión...

Como ya hemos visto, y remarca el documento que comentamos, el contexto es relevante.

Segundo: **definir cada alerta**. Se trata ahora de «transformar cada alerta en un indicador discreto y cuantificable», lo que requiere determinar exactamente qué dato o datos concreto/s habrá que utilizar para definir la alerta, cuáles son las relaciones lógicas entre los diversos datos —cuándo se utilice más de uno— y cuál o cuáles son los valores umbrales del dato o de cada uno de los datos que desencadenan la alerta.

En este paso se definirá igualmente la naturaleza y, en su caso, los valores posibles de la alerta. Así, una alerta de carácter binario sólo podrá tener dos valores: positivo o negativo —se da la situación irregular que la alerta detecta o no se da—; en cambio, un indicador de riesgo en sentido estricto podrá dar un gradiente de valores —por ejemplo valores entre 0, correspondiendo a la inexistencia de riesgo, y 10, correspondiendo al máximo riesgo—.

Tercero: **asignar a cada alerta un tipo o esquema de irregularidad, fraude o corrupción específico**. Este paso, muy ligado al anterior, implica establecer claramente cuál es el significado de la alerta.

Recordemos que una alerta no significa necesariamente una prueba plena y categórica de la existencia de una —o varias— irregularidades o supuestos de fraude o corrupción; una alerta a menudo indica que se da una circunstancia que justifica una revisión o investigación más esmerada. Eso implica tener claramente establecido qué significa la alerta, lo que determinará qué es lo que se tiene que revisar y/o investigar.

Por ejemplo, una alerta que indique la existencia de un licitador único, en el caso de una licitación donde razonablemente se espera un nivel de competencia elevado —visto el mercado y/o los precedentes— puede significar varias cosas: una errónea fijación del tipo de licitación, unos criterios de selección cualitativa de los licitadores demasiado restrictivos, la publicación del anuncio de licitación en un momento inadecuado —por ejemplo a principios o medios del mes de agosto—, una alteración coyuntural o no de la estructura del mercado, pero también la existencia de colusión entre los potenciales licitadores. Por lo tanto, en la subsiguiente revisión habrá que analizar tanto el diseño de la licitación —pliegos de cláusulas— y la tramitación del procedimiento como las características pasadas y actuales del mercado, etc.

Por otra parte, tal como acertadamente destaca el documento que comentamos, no es inusual que salten varias alertas respecto de una misma licitación o de un mismo contrato; evidentemente, en estos casos las probabilidades de que efectivamente se haya producido o se esté produciendo algún tipo de irregularidad, fraude o corrupción son más elevadas.

Cuarto: **mapear los datos de la alerta de acuerdo con el estándar OCDS**. De lo que se trata, en este paso, es de subsumir los datos concretos utilizados en cada alerta en el modelo de datos OCDS. Evidentemente este paso metodológico era ineludible para los autores del documento *Red Flags for Integrity*, vista su pretensión de establecer un listado lo más amplio y omnicomprensivo de alertas como el del documento complementario, y de definir las alertas de acuerdo con un modelo de datos y una terminología generalmente comprensibles y fácilmente aplicables para cualquier organización interesada —lo que, obviamente, llevaba a la utilización del estándar OCDS, creado por OCP—. Es igualmente evidente que este paso no es estrictamente necesario en cualquier organización que pretenda diseñar e implantar un sistema de alerta.

No obstante, el uso del estándar de datos abiertos de contratación pública OCDS se puede considerar una buena práctica que presenta interesantes beneficios: mayor facilidad a la hora de implementar las alertas que interesen de las 73 del listado del documento complementario; utilidad en la implementación de una política de datos abiertos de contratación; comparabilidad de los datos propios con las otras organizaciones nacionales o internacionales y, por lo tanto, comprobación de la validez de las alertas diseñadas con datos de otros orígenes.

Quinto: **asignar cada alerta a la correspondiente fase del ciclo de contratación**. En general se suelen distinguir cinco fases en el ciclo o proceso completo de contratación: la preparación o planificación, la licitación, la adjudicación, la formalización y la ejecución del contrato. Es pues conveniente determinar, para cada una de las alertas concretas identificadas y definidas, a cuál de aquellas fases del ciclo de contratación se refiere. Eso permite tener una visión clara de si **el sistema de alerta establecido cubre de forma homogénea y consistente todo el ciclo** de contratación, o si sólo se focaliza en alguna o algunas de las fases de lo mismo.

A este respecto es muy significativa una observación de los autores del documento *Red Flags for Integrity*: a pesar de la amplísima recopilación de posibles alertas que llevaron a cabo, constatan que «muchas más alertas se pueden calcular en las fases de licitación y adjudicación que en las de formalización, ejecución y planificación» y, por lo tanto, apuntan como posibilidad de evolución y de mejora del documento, entre otros, la incorporación de nuevas alertas centradas en la fase de planificación en la que «la teoría nos dice que existen numerosas oportunidades para actuaciones ilícitas» [70].

En este mismo sentido, es interesante traer a colación la siguiente observación del capítulo I del bloque VII de la *Guía de integridad en la contratación pública local*, publicada per la FEMP en mazo de 2019 [71]:

> *«La fase de ejecución de los contratos públicos ha sido, tradicionalmente, el pariente pobre de la contratación pública, tanto en el plano normativo como en el operativo e incluso, en cierta medida, en el doctrinal. En efecto, es notorio y por todos constatado que a la ejecución de los contratos no se le ha dedicado, ni por el legislador la ingente cantidad y detalle de normas; ni, por las administraciones —y, en especial, las locales, siempre escasas de medios—, los recursos; y hasta cabría aventurar que tampoco por la doctrina, el volumen de estudios y el rigor analítico que a la previa fase de licitación se dedican.*
>
> *[...]*
>
> *Y si consideramos ahora la praxis, la dimensión operativa de la contratación, especialmente en el ámbito local, ¿cuántas veces, [...], habremos tenido la sensación de que con la adjudicación se acababa la contratación? —cuando, obviamente, lo cierto es lo contrario: que precisamente aquél es el momento en que realmente empieza la andadura del contrato—. [...], a partir de entonces parece darse por hecho que las cosas van a ir solas, y que con dejar en manos de un técnico la conformación de las facturas y de la Intervención su fiscalización —mientras haya crédito suficiente en la partida correspondiente—, estamos al cabo de la calle.*

[70] *Op. cit.* pág. 27.

[71] Accesible en: http://femp.femp.es/files/3580-2053-fichero/GUIA_INTEGRIDAD_CONTRATACION_PUBLICA_LOCAL.pdf

Casi parecería que lo único realmente importante en un contrato público es su licitación y adjudicación; y que, a partir de ese momento, cuanto acontezca después carece de interés, son tareas materiales de menor entidad.»

Esta advertencia y puesta en guardia es perfectamente aplicable en el ámbito que nos ocupa, a la hora de diseñar un sistema de alerta: todo el ciclo de la contratación pública tiene que estar cubierto por las alertas que se implementen, y la fase de ejecución de los contratos de ninguna manera puede considerarse secundaria o menos importante, siendo especialmente críticas e importantes la identificación y recopilación de los datos de esta fase.

Para concluir esta breve referencia al documento *Red Flags for Integrity*, cuatro breves apuntes adicionales:

a. el documento insiste reiteradamente en la conveniencia y utilidad en adoptar el estándar OCDS que va mucho más allá del establecimiento de sistemas de alerta;

b. el documento, con un encomiable afán pedagógico, contiene seis ejemplos de definición de alertas concretas [72], para cada una de las cuales se define y se explica la alerta, se detallan los datos del modelo OCDS utilizados para calcularla, se incluye el algoritmo en lenguaje R —uno de los lenguajes de programación de algoritmos para el análisis y explotación de datos más usuales— para su cálculo y se incluye igualmente una explicación literal del código en lenguaje R;

c. el documento contiene igualmente una detallada explicación del contenido del documento complementario *Red Flags to OCDS Mapping*, en formato de hoja de cálculo, así como un análisis de los datos del modelo OCDS con mayor utilidad a los efectos de alertas —datos con mayor número de utilización en diferentes alertas; datos con utilidad como alertas por sí solos—; y

d. finalmente, el documento trata de recapitular las principales lecciones que se pueden extraer de la tarea realizada, identificar las carencias existentes y posibilidades de evolución y mejora, y analiza el funcionamiento de los

[72] Los 6 ejemplos de alertas tratados son los siguientes:

a. licitador único: alerta indicativa de la inexistencia de concurrencia efectiva en la licitación;

b. plazo excesivamente breve de presentación de ofertas: alerta indicativa de posible favoritismo por parte de la entidad contratante en beneficio de un licitador que dispondría de información sobre la licitación antes de su publicación;

c. licitador novel en una licitación: alerta indicativa de una alteración en el mercado de que se trate;

d. bajas mínimas en una licitación: alerta indicativa de posible colusión entre licitadores o de una errónea o irregular fijación del tipo de licitación;

e. bajas con intervalos regulares entre ellas: alerta indicativa de posible colusión; y

f. exclusión de todos los licitadores excepto del adjudicatario: alerta indicativa de posibles irregularidades en el establecimiento de los criterios de selección cualitativa de los licitadores.

sistemas de alerta realmente existentes basados en el OCDS, especialmente el de Ucrania.

En definitiva, nos encontramos ante un documento, a la vez teórico y práctico, sistemático y metodológico, enormemente pedagógico que constituye una de las mejores recapitulaciones y síntesis de la materia que nos ocupa.

4 Análisis

Hemos identificado el contexto en el cual debe situarse el presente estudio; hemos repasado el estado de situación existente; y nos hemos detenido en tres referentes insoslayables como son la herramienta Arachne, el sistema SALER y el documento *Red Flags for Integrity* de OCP.

Llegados a este punto, estamos en condiciones de desarrollar algunas reflexiones y consideraciones que consideramos relevantes.

4.1 Prevención y contingencia

Tal y como acertadamente destacan Roger FOLGUERA FONDEVILLA y Lara BAENA GARCÍA en su artículo monográfico ya citado [73], una buena gestión integral de los riesgos de irregularidades, de fraude o de corrupción tiene que incluir dos perspectivas o dimensiones: la preventiva y la contingente.

La **actuación preventiva** tiene como objetivo reducir la probabilidad de que los riesgos para la integridad en una institución se produzcan efectivamente, se materialicen, mientras que la **actuación contingente**, por el contrario, se centra en reducir el alcance y la gravedad de los daños y perjuicios producidos cuando los riesgos se han llegado a materializar.

Pues bien, al respecto el documento *Red Flags for Integrity* apunta una idea disruptiva en el ámbito que consideramos: **la capacidad de los sistemas de alerta basados en el análisis de datos de hacer converger ambos paradigmas, el preventivo y el contingente**.

Hemos visto cómo los sistemas de alerta permiten detectar las posibles irregularidades y los riesgos potenciales de fraude y corrupción antes de que se lleguen a materializar; en este sentido, el documento *Red Flags for Integrity* insiste, como hemos destacado, en el carácter intrínsecamente proactivo de estos sistemas de alerta [74].

Esta afirmación debe sin embargo matizarse: el elemento clave aquí es la capacidad de explotar los datos de contratación pública ***en tiempo real***.

Efectivamente, hay que distinguir entre sistemas de alerta basados en el análisis de datos que funcionan en tiempo real, analizando los datos y, en su caso, generando las alertas correspondientes a medida que se generan los datos, en cada trámite y fase del correspondiente procedimiento de contratación, y sistemas de alerta basados en datos que funcionan *a posteriori*, analizando los datos y generando las alertas con posterioridad —más o menos lejos en el

[73] *Op. cit.* nota 6 anterior.

[74] Cfr. apartado 3.3.1 anterior (págs. 52 y 53) y notas 65 y 66.

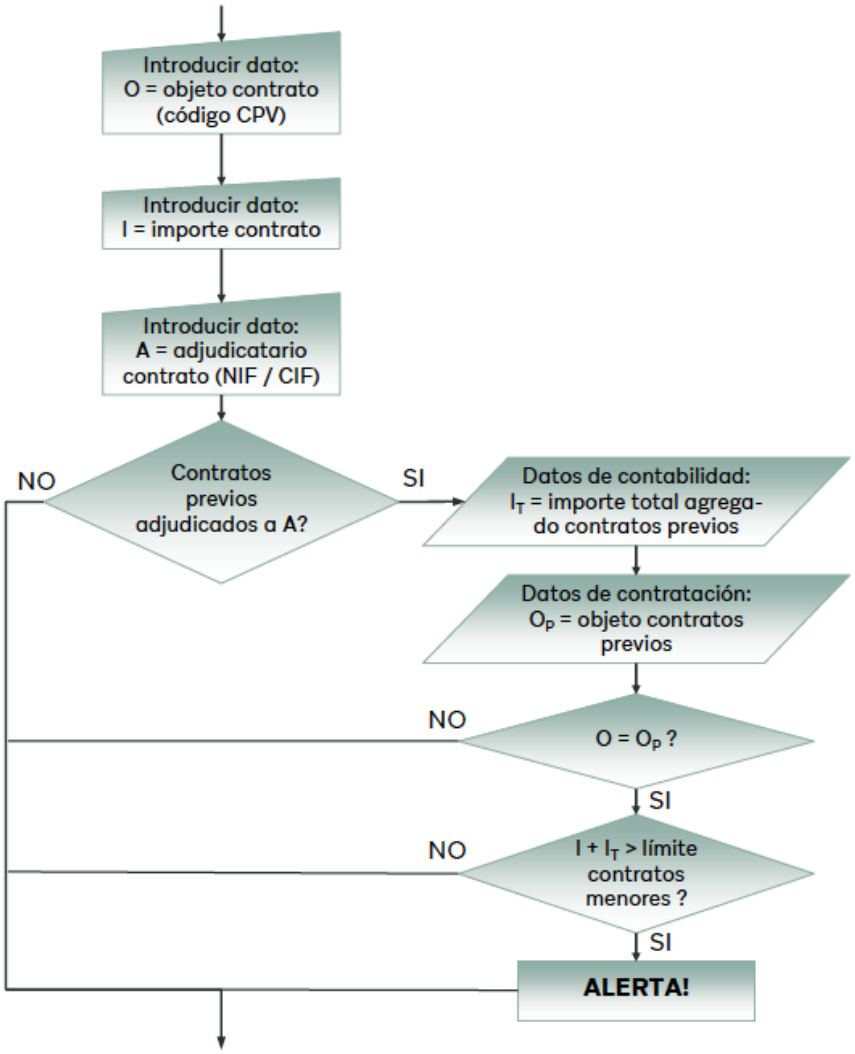
tiempo— a la realización de los acontecimientos que, datificados, generan los datos utilizados.

En el primer caso, prevención y contingencia convergen: el hecho de que la alerta permita detectar la irregularidad en el momento en el cual se produce **permite igualmente evitarla** y, por lo tanto, **reducir a cero los daños o perjuicios causados**. En el segundo caso, obviamente, las alertas que permiten la detección de irregularidades, fraude o corrupción *a posteriori* son, paradigmáticamente, instrumentos de actuación contingente.

Ilustramos esta idea con un ejemplo: el fraccionamiento de contratos con el fin de eludir los procedimientos de contratación con publicidad y concurrencia.

Un sistema de alerta puede obtener, de fuentes internas o de fuentes abiertas —datos abiertos de contratación— la relación de contratos menores y/o de contratos adjudicados sin ningún procedimiento con publicidad y concurrencia y, analizando estos datos, detectar los casos en los cuales se han producido varias adjudicaciones al mismo contratista de contratos con objeto idéntico o parecido, en un corto periodo de tiempo —pongamos un año—, de manera que el importe total agregado de aquellas diversas adjudicaciones a un mismo contratista supere significativamente los límites de la contratación menor. Eso tendría que desencadenar una alerta de fraccionamiento: existen indicios —no necesariamente pruebas concluyentes; estas se tendrían que obtener mediante la revisión o investigación que la alerta tendría que desencadenar— de que se ha fraccionado la prestación de que se trate en varios contratos para poder adjudicarlos todos a un mismo contratista, eludiendo los requisitos normativos de publicidad y concurrencia. Estamos ante un mecanismo contingente: el riesgo —que se produzca fraccionamiento— ya se ha materializado, y, si se verifica que efectivamente se ha producido fraccionamiento ilegal, es decir, que no existen razones excepcionales, legalmente admitidas y previstas, que justifiquen aquella situación, lo único que se podrá hacer es llevar a cabo actuaciones para revertir las situaciones ilegales producidas —la revisión de oficio de las adjudicaciones de los contratos, por ejemplo—, minimizar los daños producidos —suspender en su caso los contratos no totalmente ejecutados; imponer sanciones o penalizaciones— y, como mínimo, evitar su perpetuación o reproducción en el futuro —reforzar los medios de control interno; depurar responsabilidades—.

Ahora bien, podemos igualmente concebir un sistema de alerta, necesariamente basado en datos internos —si tenemos que esperar a la publicación de los datos, será demasiado tarde y nos encontraremos en el escenario anterior—, que detecte, en el momento en que se vaya a producir la adjudicación de un contrato, la acumulación de contratos con el mismo objeto —o un objeto *a priori* coincidente: mismo código CPV— en el mismo contratista por un importe agregado que supere los límites de la contratación menor. El mecanismo, descrito en términos de un diagrama de flujo, se podría representar, simplificadamente, de la manera siguiente:



Con un sistema como éste [75], es posible, en los casos en que se produzca la alerta, adoptar medidas para evitar que el riesgo de fraccionamiento llegue a materializarse.

Pero, ¿qué medidas? Aquí las opciones son diversas, y dependen de criterios y decisiones de gestión que no pueden fijarse de manera categórica y general, puesto que dependerán, en gran medida, de las posibilidades y características organizativas de cada entidad. Veamos algunas:

a. una primera opción, muy radical, es que cuando salte la alerta el sistema simplemente no permita la adjudicación del contrato al adjudicatario inicialmente previsto: sencillamente el sistema —el gestor electrónico de expedientes de contratación— no lo permite y, por lo tanto, el servicio gestor del expediente tendrá que buscar a otro contratista a quien adjudicar aquel contrato —o desistir de la contratación, claro está—;

b. pero también es posible que en estos casos el sistema exija al servicio gestor un informe adicional justificando las razones y los fundamentos legales que justificarían la adjudicación del contrato al contratista

[75] Según la información de que disponemos el Ayuntamiento de Santa Coloma de Gramenet dispone de un sistema muy parecido al que se describe en este ejemplo.

inicialmente previsto —por ejemplo la inexistencia de competencia respecto de la prestación objeto del contrato por razones técnicas o de protección de derechos exclusivos, *ex* art. 168 a) 2.° de la LCSP—;

c. también es posible que el sistema permita la adjudicación y que la alerta dé lugar a una revisión o auditoría, por los órganos de control internos del ente de que se trate, de todos los expedientes de contratación adjudicados a la misma empresa; en este caso, el mecanismo de alerta tendría un carácter más contingente que efectivamente preventivo.

Las posibilidades son numerosas y es difícil establecer apriorísticamente y con carácter general una única opción como correcta. En este sentido, la opción radical antes apuntada —el sistema impide categóricamente y sin alternativas la adjudicación del nuevo contrato al adjudicatario previsto— puede generar situaciones de bloqueo y disfunciones en administraciones con déficits de capacidad de gestión que den lugar a problemas más graves que los que se pretenden evitar.

No obstante, el hecho es que los sistemas de alerta abren posibilidades reales de incidir en tiempo real sobre los riesgos potenciales y, en este sentido, hacen converger y aproximarse, como hemos dicho, los dos grandes paradigmas, prevención y contingencia, de la gestión de los riesgos de irregularidades, fraude y corrupción.

4.2 Sistemas externos vs. internos

El ejemplo del apartado anterior nos lleva a una segunda reflexión, centrada en la distinción entre sistemas de alerta que designaremos como *internos* y *externos*, de acuerdo con las definiciones siguientes:

a. designaremos como **sistemas externos** los sistemas de alerta que funcionan con datos obtenidos de fuentes diferentes al propio gestor electrónico de expedientes de contratación y que, por lo tanto, no tienen *a priori* capacidad para interactuar en tiempo real, directa y automatizadamente, con éste —o, si la tienen, es más o menos limitada—; y

b. designaremos como **sistemas internos** los sistemas que obtienen los datos directamente del gestor electrónico de expedientes de contratación y pueden interactuar con este en tiempo real.

Esta distinción es relevante en la medida en que muchos —probablemente la mayoría— de los proyectos y estudios sobre sistemas de alerta se basan en datos abiertos [76] y, por lo tanto, se configuran más como sistemas contingentes que como sistemas realmente preventivos.

Efectivamente, el hecho de que un sistema de alerta se nutra de datos abiertos, tanto si los datos se obtienen ya estructuradas y directamente explotables de un portal de transparencia o de datos abiertos, o del RPC, como si se obtienen

[76] Éste es el caso, entre muchos otros, del proyecto *DIGIWHIST, The Digital Whistleblower* así como del proyecto húngaro *Red Flags*, ya mencionados. Cfr. apartado 1.3 anterior (pág. 8) y notas 2 y 3.

mediante técnicas de *scraping*[77] y, eventualmente, son posteriormente objeto de estructuración y depuración para su ulterior tratamiento, introduce inevitablemente un retraso que imposibilita que la alerta incida en tiempo real en la tramitación del procedimiento de contratación y, por lo tanto, limita la eficacia del sistema a la vertiente contingente: el sistema permitirá detectar irregularidades una vez ya se hayan producido, pero sólo indirectamente y con carácter prospectivo permitirá evitar que se produzcan; lo que ha pasado ha pasado —las irregularidades detectadas a partir del análisis de los datos— y ya sólo se podrá plantear evitar que se perpetúe o se reproduzca mediante la adopción o implementación *a posteriori* de medidas correctoras.

A este respecto hay que tener presente, si consideramos un sistema de alerta que obtenga los datos del RPC, que el plazo para la comunicación de los datos al Registro es de un mes desde la fecha de formalización del contrato o desde la fecha de la aprobación de la modificación, prórroga, incidencia, conclusión o liquidación[78]. La imposibilidad de una reacción en tiempo real es pues evidente. Y si consideramos un hipotético sistema de alerta basado en datos obtenidos mediante *scraping* de la PSCP, probablemente podremos acortar el tiempo de reacción pero es igualmente evidente que subsiste en gran medida la imposibilidad de incidir en tiempo real en la tramitación del procedimiento —sin contar los problemas añadidos derivados del proceso mismo de obtención de los datos por aquella vía—.

La **superioridad de los sistemas internos** es pues, desde este punto de vista, indiscutible. Y por lo tanto sería deseable centrar los esfuerzos en el desarrollo de sistemas de alerta de carácter interno que se nutran de datos directamente obtenidos de los gestores electrónicos de expedientes —lo que evidentemente sólo será posible si se dispone de un gestor integrado que cubre todo el procedimiento de contratación; si una parte del procedimiento no está automatizada ni, por lo tanto, datificada, la limitación estructural es evidente— y se diseñen con capacidad para interactuar automatizadamente con el gestor de expedientes, para garantizar el efecto realmente preventivo de las alertas.

De esta idea podemos derivar dos corolarios, uno muy concreto y otro de mucho más general.

Concretamente, si consideramos de nuevo la iniciativa del Consorcio Localret para dotar los entes locales de una herramienta de seguimiento, control y planificación de la contratación, ya comentada[79], recordemos cómo el informe

[77] El ***scraping*** es la técnica consistente en la extracción automatizada, mediante un programa *ad hoc*, de datos accesibles y legibles, normalmente en una página web; dicho en otras palabras, se trata de extraer automatizadamente los datos de una determinada fuente, lo que da como resultado una base de datos, p. ej. un archivo en formato Excel. El hecho que la base de datos se obtenga mediante aquel proceso implica que a menudo los datos así obtenidos presenten errores o lagunas lo que determina que sea necesario, antes de su explotación, proceder a la su depuración —eliminación de redundancias, corrección de errores o inconsistencias, estructuración y homogeneización, etc.—, y, en general, sean de menor calidad.

[78] Así lo prevé el art. 3 de la Orden ECO/47/2013, de 15 de marzo, por la cual se regula el funcionamiento y se aprueba la aplicación del Registro público de contratos de la Generalitat de Cataluña.

[79] Cfr. apartado 2.3.3 anterior (págs. 35 y ss.).

sobre los resultados de la consulta de mercado llevada a cabo recogía, en relación, específicamente, a la obtención de los datos, la distinción que ahora consideramos, entre soluciones integradas de contratación electrónica, que obtienen los datos «directamente del tramitador de expedientes o de la herramienta de licitación electrónica» —soluciones internas—, y soluciones específicas no incluidas en una herramienta de contratación electrónica, que «obtienen los datos (de los contratos) desde las plataformas públicas de contratación: PLACE y/o PSCP […] o también del Registro Público de Contratos (RPC)» —soluciones externas—.

Pues bien, en la medida de lo posible sería deseable que se apostara y se favorecieran especialmente las primeras de aquellas soluciones, de carácter interno, especialmente de cara a la implementación en las mismas de un sistema automatizado de alerta.

Y si consideramos ahora la disyuntiva que nos ocupa desde una perspectiva mucho más general, no podemos dejar de apuntar un riesgo inherente a la idea misma de los sistemas externos de alerta, que es la siguiente.

Ya hemos señalado como la idea de utilizar los datos abiertos de contratación como instrumento de lucha contra la corrupción es un paradigma globalmente consolidado [80]. Y acabamos de ver cómo muchos de los proyectos de sistemas de alerta responden a este paradigma basándose precisamente en datos abiertos o en datos obtenidos de las plataformas de contratación electrónica.

Pues bien, sin cuestionar en absoluto la afirmación de que «los datos abiertos contribuyen a la prevención, la detección, la investigación y la reducción de la corrupción» [80], en los trabajos de elaboración del presente estudio hemos podido detectar el riesgo difuso de **una invocación desviada de aquel principio** que se concretaría en la idea de priorizar y centrar todos los esfuerzos en la transparencia y la implementación de datos abiertos, asumiendo implícitamente que eso, en la medida en que posibilita y favorece el desarrollo de sistemas de alerta de carácter externo, da satisfacción al objetivo de desarrollar sistemas de alerta basados en datos.

Y evidentemente no es así.

Los sistemas de alerta basados en datos no tienen que concebirse como una finalidad en sí misma, sino como **un instrumento de control al servicio de la integridad**. Y el primero y principal nivel de control, en toda organización y especialmente en el sector público es el **control interno**. Rehuir las responsabilidades y el fortalecimiento del control interno porque existe o puede existir un control externo es absurdo y perverso: es evidente que **donde deben implementarse los mecanismos y los instrumentos más eficaces y eficientes de detección de irregularidades y de potenciales fraudes y corrupciones es en el ámbito interno**, como herramientas al servicio de las instancias de control

[80] *Principios de datos abiertos anticorrupción*, aprobados por el G20 en 2015, ya citados. Cfr. apartado 2.1.2 anterior y nota 16 (pàg. 17).

interno, especialmente cuando estas instancias disponen de recursos y medios limitados o insuficientes, como es a menudo el caso en el ámbito local.

4.3 Tipología: 3 niveles de sistemas de alerta

Hemos visto como el documento *Red Flags for Integrity* de OCP destacaba especialmente el interés de analizar conjuntamente, cruzándolos, tanto los datos de contratación pública, en sentido estricto, como otros tipos de datos —si bien obviamente relacionados con la contratación— como serían datos mercantiles, financieros, de titularidades reales de empresas, de vinculaciones entre entidades, etc.

Esta importante idea nos permite establecer una **tipología de los sistemas de alerta**, distinguiendo **3 niveles** que, en orden creciente de capacidad de detección de irregularidades, fraudes y corrupción, serían los siguientes:

4.3.1 Nivel 0: el gestor electrónico de expedientes

Todo gestor electrónico de expedientes de contratación, adecuadamente diseñado y configurado, puede **cumplir la función y servir como sistema automatizado de alerta** y prevenir que se materialicen algunos tipos de irregularidades. Efectivamente, si presuponemos un diseño correcto y una configuración conforme con los requisitos e imperativos legales, el gestor de expedientes estructura y articula la tramitación del procedimiento de acuerdo con el marco legal, impidiendo o bloqueando la tramitación —o, como mínimo, generando una alerta— si en algún punto no se cumplen los requisitos legales o no se respetan los trámites.

Así, por ejemplo, si no se carga en el gestor el informe o el acuerdo motivando la necesidad del contrato que prevé el art. 116.1 de la LCSP, con el contenido estipulado en el apartado .4 de aquel precepto, o si no se cargan los documentos exigidos por su apartado .3, el gestor no debería permitir pasar al trámite siguiente, de aprobación del expediente —art. 117.1 de la LCSP—.

Ahora bien, el gestor electrónico de expedientes de contratación, como sistema de alerta, presenta **limitaciones muy importantes** en la medida que puede garantizar el cumplimiento *puramente formal* del procedimiento pero no el cumplimiento sustancial del marco legal —p. ej. difícilmente detectará que un informe preceptivo contenga errores burdos o esté vacío de contenido—.

Por otra parte, la eficacia y la utilidad de determinadas alertas, implementadas a este nivel básico en el gestor electrónico de expedientes de contratación, resulta muy relativa —e incluso puede llegar a ser nula—. Efectivamente, determinadas circunstancias que constituyen indicadores objetivos de riesgo pueden ser, aisladamente consideradas, plenamente compatibles con el marco legal y, por lo tanto, *a priori*, no deberían determinar la detención de la tramitación en curso; y si dan lugar a una alerta probablemente se la tenga que descartar como falso positivo.

En este sentido y a título de ejemplo, el hecho que en una licitación por procedimiento abierto, con toda la publicidad legalmente exigible y un plazo

suficiente de presentación de ofertas, se presente única oferta puede ser indicativo de varios riesgos: una licitación a medida o un acuerdo colusorio entre potenciales licitadores; pero si la oferta es conforme con las exigencias del pliego de cláusulas y racional y razonable, *a priori* el contrato se tendría que adjudicar.

Y, sobre todo, la principal limitación del gestor de expedientes como sistema de alerta es que sólo puede tener en cuenta los datos del procedimiento concreto que se está tramitando, lo que impide detectar irregularidades que se articulan mediante un conjunto de procedimientos, legales aisladamente considerados pero irregulares —o incluso delictivos— considerados en conjunto: paradigmáticamente, este sería el caso del fraccionamiento ilegal de contratos. Esta consideración nos lleva al siguiente nivel de un sistema de alerta.

4.3.2 Nivel 1: explotación de los datos de contratación y de contabilidad

Para superar estas limitaciones es necesario que el sistema de alerta tenga acceso y explote no sólo los **datos del procedimiento concreto que se está tramitando** sino igualmente, y de forma simultánea, los **datos de toda la contratación pública** del ente que se trate así como los **datos contables correspondientes** —que, de hecho, son la vertiente cuantitativa, el reflejo económico de la contratación—.

En este nivel el sistema de alerta **articula la interacción entre el gestor de expedientes y las bases de datos de contratación y contabilidad** que contienen información, que va más allá del concreto procedimiento que se está tramitando.

El ejemplo que hemos presentado anteriormente [81] de una posible alerta que detecte el fraccionamiento de contratos con el fin de eludir los procedimientos de contratación con publicidad y concurrencia ilustra perfectamente esta idea. En el diagrama de flujo que describe el funcionamiento de aquella alerta se ve claramente como los datos del contrato concreto que se está tramitando —importe, I, y objeto, O— se comparan con los datos extraídos de la contabilidad —importe total agregado, I_T, de los contratos adjudicados al contratista al cual se pretende adjudicar el contrato que se está tramitando— y de la contratación anterior del ente considerado —objeto, O_P, de los contratos previamente adjudicados al mencionado contratista—.

Es importante indicar que el GEEC, que como hemos visto [82], tiene prevista normativamente su integración con los sistemas económicos y financieros corporativos de la Generalitat de Cataluña (GECAT y Pangea), el RPC, la PSCP y otras bases de datos, plataformas y sistemas, soportaría por lo tanto sin requerir adaptaciones sustanciales un sistema de alerta de este nivel.

[81] Cfr. apartado 4.1 anterior (págs. 61 y ss.).

[82] Cfr. apartado 2.3.1 anterior (págs. 28 y ss.).

En cuanto a la herramienta de seguimiento, control y planificación para los entes locales objeto de la iniciativa del Consorcio Localret [83], hemos visto igualmente cómo se prevé la obtención de datos directamente de los gestores de expedientes en caso de soluciones integradas de contratación electrónica o de las plataformas públicas de contratación y del RPC en el caso de soluciones no integradas —obviamente como ya hemos indicado en el apartado 4.2 anterior, menos interesantes—. Tratándose de una iniciativa todavía en curso de desarrollo sería especialmente interesante favorecer las soluciones que no sólo incorporen el acceso a los datos de contratación sino igualmente a las de contabilidad.

Ahora bien, una rápida ojeada a las alertas detalladas en el listado complementario en el documento *Red Flags for Integrity* permite constatar que el cruce de los datos de un concreto procedimiento en tramitación con los datos de contratación y de contabilidad de la entidad contratante, aunque permite detectar numerosas alertas, presenta igualmente limitaciones: muchas otras alertas requieren otros datos que, *a priori*, no constan en aquellas dos bases de datos, como, ejemplo de nuevo paradigmático, las vinculaciones entre empresas licitadoras.

Eso nos lleva al siguiente nivel de los sistemas de alerta.

4.3.3 Nivel 2: cruce con otros datos internos y externos

El modelo de los sistemas de alerta de este nivel son los dos referentes que hemos estudiado: la herramienta Arachne de la Comisión Europea y el sistema SALER de la Comunidad Valenciana.

En este nivel, el sistema de alerta se nutre y explota **datos de tres fuentes**:

a. los datos del gestor electrónico de expedientes de contratación, referidos al procedimiento concreto que se está tramitando;

b. los datos de contratación y de contabilidad de la entidad considerada, de carácter interno —eso, en todo caso, es lo deseable, aunque eventualmente, a falta de una mejor opción, se pueda plantear, como hemos visto, la obtención de los datos de contratación de fuentes externas: PSCP, RPC u otros—; y

c. datos adicionales de carácter externo: datos mercantiles —del Registro Mercantil—, de solvencia —RELI, por ejemplo—, de nombramientos en cargos públicos o privados, datos económicos y financieros —bases de datos de información económica de sociedades—, e incluso —tal como hemos visto que prevé la regulación del sistema SALER— datos abiertos de Internet.

Evidentemente, este es el nivel idóneo y, por lo tanto, en el que tendría que aspirar a situarse el diseño y proyecto de implementación de cualquier sistema de alerta. No obstante, no podemos obviar algunas problemáticas relevantes que se plantean a este nivel.

[83] Cfr. apartado 2.3.3 anterior (págs. 35 y ss.).

La primera hace referencia a la **complejidad del sistema**. En este nivel, desde un punto de vista técnico, el sistema de alerta excede claramente lo que es un gestor electrónico de expedientes de contratación, propiamente dicho. El sistema de alerta difícilmente se puede plantear como parte del gestor de expedientes, sino que más bien se tiene que concebir como un sistema autónomo.

En efecto, la interacción de un gestor de expedientes con los datos de contratación y de contabilidad, y su integración con los sistemas de gestión financiera, económica y contable es algo que ya existe —el GEEC de la Generalitat de Cataluña es un ejemplo, pero existen igualmente muchas otras soluciones integradas que ofrecen esta posibilidad—; y, por lo tanto, la implementación de sistemas de nivel 1 no plantea, *a priori*, grandes problemas técnicos.

Ahora bien, cuando consideramos sistemas de nivel 2, que tienen que interaccionar con bases de datos externas y eventualmente explotar datos abiertos la situación es diferente: estamos hablando de sistemas de alerta que, obviamente, interactúan con el gestor de expedientes pero que constituyen técnicamente un sistema diferente. Aunque este tipo de sistemas son, a nuestro entender, el objetivo a alcanzar, los retos técnicos a este nivel son ciertamente mucho más importantes.

En este nivel el principal reto reside en el **grado de compromiso de las instituciones con la integridad**. En el contexto en el cual nos encontramos, cualquier impulso a la digitalización de las administraciones públicas tendría que incorporar la integridad como principio nuclear esencial. Todos los desarrollos digitales para el sector público tendrían que incorporar el **principio de *integridad por diseño*** en su concepción e implementación y, por lo tanto, incorporar mecanismos de detección y prevención de riesgos para la integridad no como una opción complementaria sino un elemento integrante de la estructura principal vertebradora de toda solución tecnológica para el ámbito de la contratación pública. Este principio general tendría que ser inspirador y director de cualquier actuación o desarrollo en este ámbito.

La segunda problemática que se plantea a este nivel se refiere a la cobertura jurídica, desde el punto de vista del marco legal de **protección de datos personales**, del **uso de los datos en los sistemas de alerta** de este nivel. Efectivamente, una de las alertas más importantes y transversales a todo el ciclo de la contratación pública —en la medida en que corresponde a un riesgo que se puede dar en cada una de las fases de la contratación: preparación o planificación, licitación, adjudicación, formalización y ejecución del contrato— es la de detección de posibles conflictos de interés y, evidentemente, la implementación de esta alerta necesariamente comporta la explotación y el tratamiento de datos personales.

Analizada la cuestión desde esta perspectiva, no parece que el uso de los datos personales del propio procedimiento de contratación plantee ningún problema, vista la previsión del art. 6 c) del RGPD y su transposición en el art. 8.1 de la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los

derechos digitales (LOPDGDD), que habilita al tratamiento de los datos para el cumplimiento de una obligación legal, puesta en relación con el imperativo de prevención de los conflictos de intereses del art. 64 de la LCSP. Tampoco parece que plantearía problemas el uso de datos personales que consten en registros públicos con finalidad de publicidad y propósito general, como sería el caso del Registro Mercantil. El uso de datos personales de otros expedientes de contratación —extraídos por el sistema de alerta de la correspondiente base de datos— igualmente se podría entender —si bien no resulta tan evidente— amparado por las referidas previsiones legales. Pero parece claro que el uso de datos abiertos obtenidos de Internet requeriría una habilitación legal específica, de acuerdo con lo que prevé el arte. 8.3 de la LOPDGDD.

En este sentido, sería deseable poder **contar con una previsión normativa expresa de rango legal** —idealmente en la LCSP o eventualmente en la normativa catalana de desarrollo de la misma—, de la misma manera que el sistema SALER se encuentra amparado por las previsiones del art. 17.3 de la Ley 22/2018 [84].

La tercera problemática —y quizás la más importante— hace referencia a los **recursos que hace necesaria la existencia misma de un sistema de alerta**, especialmente si es un sistema del máximo nivel y, por lo tanto, tiene una gran capacidad de detección de varios tipos de posibles irregularidades.

Efectivamente, a medida que se incrementa el nivel de un sistema de alerta y crece, por lo tanto, su capacidad de detección de irregularidades, fraudes y corrupción, se vuelve más y más crítico disponer de recursos para gestionar las alertas generadas. Si consideramos alertas que no comportan un bloqueo automático de la tramitación del expediente y que no indican inequívocamente la existencia de una irregularidad, sino una alta probabilidad —pero no la certeza— de materialización de un riesgo, es evidente que implementar un sistema de alerta sin dotar en el órgano responsable de la gestión y explotación del sistema de unos mínimos recursos no tiene ningún sentido. Las alertas tienen utilidad si permiten reaccionar en tiempo real. Pero si la falta de medios impide cualquier tipo de reacción, o sólo permite reacciones *a posteriori* en forma de constatación de los perjuicios causados, ya irreversibles, el sistema de alerta prácticamente no sirve para nada.

Por lo tanto, sea del nivel que sea pero especialmente si es de alto nivel, la implantación de un sistema de alerta tiene que ir acompañada del estudio de dimensionamiento y de la correspondiente adscripción de los recursos necesarios para garantizar la utilidad y la efectiva atención, gestión y seguimiento de las alertas que el sistema pueda generar.

4.4 Metodología: del mapa de riesgos a los elementos de un sistema de alerta

Llegados a este punto de nuestro estudio, parece adecuado recapitular y sintetizar las ideas, criterios, indicaciones y elementos metodológicos que hemos repasado hasta aquí.

[84] Cfr. apartado 3.2 anterior (págs. 49 y 50).

No se trata propiamente de elaborar una guía metodológica para el diseño e implementación de un sistema de alerta, pero sí de establecer unas indicaciones básicas sobre los aspectos principales a tener en cuenta.

El punto de partida y premisa principal es la primera de las ideas clave apuntadas en el documento *Red Flags for Integrity*: **el contexto lo es todo**.

Un sistema de alerta operativo y eficaz no se diseña en abstracto sino en un determinado contexto y, por lo tanto, el primer paso metodológico es la **identificación de las alertas relevantes y útiles**, de todas las posibles, teniendo en cuenta las especificidades y singularidades de la organización donde se pretenda implementar el sistema de alertas y del marco legal y operativo existente.

En este primer paso parece evidente que los **órganos de control interno** tienen que jugar un rol importante: son los que tienen la más certera, detallada y fiable información y percepción de las debilidades y disfunciones de la organización y de las irregularidades que se han producido, se producen y se pueden producir. En este sentido, el historial de reparos formulados por la Intervención constituye una valiosa fuente de información.

Este primer paso consiste de hecho, en gran medida, en el **proceso de identificación, análisis y evaluación de los riesgos** que constituye el objeto de una parte importante de los materiales del proyecto *Riesgos para la integridad en la contratación pública* de la Oficina Antifraude, ya mencionado [85]. Por lo tanto, muchos de los documentos y herramientas producidos en el marco de aquel proyecto serán de gran utilidad para llevar a cabo correctamente este primer paso metodológico en el diseño de un sistema de alertas.

El segundo paso metodológico es **definir cada alerta** concreta, lo que comporta diferentes operaciones conceptuales y organizativas:

a. por una parte, determinar exactamente qué **datos concretos** son necesarios para definir la alerta, cuáles son las **relaciones lógicas entre los diversos datos** cuando sea más de uno —para esta operación será de una enorme utilidad el documento complementario de OCP con el listado de 73 posibles alertas— y cuál o cuáles son los **valores umbrales** del dato o de cada uno de los datos que desencadenan la alerta;

b. por otra parte, determinar de dónde se pueden extraerse los datos necesarios, es decir, identificar las diversas **fuentes de datos**, tratando de priorizar el acceso directo a datos de carácter interno respecto de datos externos —la idea rectora en este punto es la ya apuntada de la **superioridad de los sistemas internos sobre los externos**, pero evidentemente eso no será siempre posible—, lo que comporta analizar y evaluar cuestiones como la **disponibilidad y calidad de los datos**, y, cuando se trate de datos personales, las posibilidades de su tratamiento

[85] Cfr. apartado 1.1 anterior (pág. 6) y nota 1.

teniendo en cuenta el régimen normativo aplicable en materia de **protección de datos**;

en este punto, el hecho de tener **mapeados los datos de acuerdo con el estándar OCDS** puede ser útil y conveniente desde varios puntos de vista, como ya hemos señalado, aunque no sea estrictamente necesario;

c. es igualmente necesario interpretar correctamente el significado de la alerta, lo que implica:

   i. asociarla a un concreto supuesto o esquema de i**rregularidad, fraude o corrupción**;

   ii. determinar la **naturaleza de la alerta**: si se trata de una alerta que da información inequívoca sobre la existencia cierta de una irregularidad, fraude o corrupción, o de una alerta que sólo facilita una información indiciaria sobre la posibilidad —pero no la certeza— de la existencia de una irregularidad, fraude o corrupción; y en este segundo caso, hay que determinar si el valor de la alerta aporta información sobre la probabilidad, baja, media o alta de la materialización del riesgo de que se trate.

Otro elemento importante de este segundo paso metodológico de definición de las alertas concretas del sistema, que tiene un carácter continuado en el tiempo y probablemente iterativo, es la **revisión y mejora continúa de cada alerta**: una vez diseñada e implementada la alerta, hay que analizar periódicamente y de forma continuada su funcionamiento, para detectar si este es correcto y eficaz. Parece evidente que una alerta que genera constantes falsos positivos, o, al contrario, que prácticamente no salta nunca, razonablemente o está mal diseñada o quizás no es realmente útil: hace falta determinar por qué pasa eso y llevar a cabo, si procede, los ajustes adecuados tanto en el diseño mismo de la alerta como de los valores umbrales del o de los datos en que se basa. Idealmente, una alerta está óptimamente diseñada y es eficaz cuando sólo salta si realmente se está materializando o se puede materializar con total certeza el riesgo que está diseñada para detectar.

Otro paso metodológico, muy próximo a lo que acabamos de considerar, es **asignar cada alerta a la correspondiente fase del ciclo de contratación**, para determinar que el sistema de alerta —el conjunto de alertas concretas— cubre homogéneamente todo el ciclo de contratación, sin que haya "puntos ciegos" donde se puedan materializar los riesgos sin que el sistema lo detecte.

Finalmente, un último paso metodológico, muy importante, de carácter organizativo, es **definir el tratamiento y los efectos de la alerta** y, a estos efectos, asignar, si procede, los recursos necesarios. Eso implica:

a. definir —probablemente a nivel normativo, como mínimo a nivel normativo interno— los **efectos de la alerta**: como ya hemos visto [86], las posibilidades son muy diversas, y pueden ir desde el bloqueo total y paralización de la tramitación del procedimiento hasta simplemente la constancia en un registro de que se ha producido la alerta;

[86] Cfr. apartado 4.1 anterior (págs. 62 y 63).

b. si la alerta no es indicativa inequívocamente de la materialización efectiva o inminente de un riesgo, pero sólo indicativa indiciariamente de una probabilidad de la misma, hace falta determinar qué **actuaciones de verificación o investigación** se llevarán a cabo para confirmar o descartar la existencia, real o potencial del riesgo, y quien llevará a cabo estas actuaciones;

c. cuando la alerta tenga carácter puramente contingente y, por lo tanto, indique la materialización de un riesgo, es necesario, igualmente, definir las actuaciones adecuadas para **revertir** —cuándo sea posible— **la situación irregular o fraudulenta** producida, llevar a términos las **actuaciones disciplinarias y de depuración de responsabilidades** adecuadas y, evidentemente, diseñar e implementar las **medidas de prevención** necesarias para evitar la perpetuación o reproducción en el futuro de la materialización del riesgo.

Para acabar trataremos de referir de manera concreta estos elementos metodológicos a algunas de las alertas correspondientes a los principales riesgos en el ciclo de la contratación pública identificados en el documento de trabajo n° 3 del proyecto *Riesgos para la integridad en la contratación pública* de la Oficina Antifraude [87].

En el cuadro de las páginas siguientes se identifican algunos de estos riesgos, siguiendo el orden lógico de las fases del ciclo de contratación pública: preparación, licitación, adjudicación y formalización, ejecución, indicando para cada uno:

a. el riesgo de que se trata;

b. la fase del ciclo de contratación en el cual se sitúa;

c. la descripción de la irregularidad concreta y/o del supuesto de fraude o corrupción correspondiente;

d. la descripción literal de la alerta;

e. una relación literal de los datos en los cuales se basa;

f. la tipología de estos datos, según la clasificación que ya hemos utilizado[88]: datos del procedimiento —en principio directamente recopilables del

[87] Cfr. nota 1 anterior. Este documento de trabajo, titulado *Identificación de riesgos. 12 áreas de riesgos de irregularidades, fraude o corrupción que evaluar*, puede consultarse en la web de la Oficina Antifraude en: https://www.antifrau.cat/sites/default/files/Documents/Recursos/DT03_riesgos-integridad-contratacion-publica-identificacion-riesgos.pdf.

Existen muchas y muy diversas taxonomías o clasificaciones de los riesgos de corrupción en el ciclo de la contratación pública. La del mencionado documento de la Oficina Antifraude es una de las posibles, que coincide bastante con la que podemos hallar en el documento de la OCDE *Analytics for Integrity —op. cit.* apartado 1.2, *Overview of corruption and fraud risks across the infrastructure project cycle* (*Resumen de los riesgos de corrupción y fraude en el ciclo de los proyectos de infraestructuras*), págs. 10 a 13, y anexo 1.A, págs. 20 a 26—. El documento *Red Flags for Integrity* utiliza una clasificación diferente, basada, como ya hemos visto, en la de la *Guía para la lucha contra la corrupción y el fraude en los proyectos de desarrollo* (*Guide to Combating Corruption & Fraud in Development Projects*) —cfr. nota 68 anterior—.

[88] Cfr. apartado 4.3 anterior (págs. 66 y ss.).

gestor electrónico de expedientes de contratación—, datos de contratación y de contabilidad de la entidad contratante, y datos adicionales de carácter externo: de otras bases de datos y datos abiertos de Internet;

g. si la alerta hace uso de datos de carácter personal;

h. el tipo o naturaleza de alerta: si da información concluyente o meramente indiciaria sobre la existencia de irregularidades, fraude o corrupción;

i. el nivel de la alerta de acuerdo con la tipología definida en el apartado 4.3 anterior; y

j. una indicación muy aproximada sobre la complejidad del diseño e implementación de la alerta, basada principalmente en la necesidad de explotar conjuntamente varios datos para la misma alerta, el tipo de datos y el soporte en que se encuentran —así, a título de ejemplo, el uso de datos cuantitativos o definidos inequívocamente con un número cerrado de posibles valores en campos concretos del gestor de expedientes presenta menos complejidad que el uso de datos de carácter textual en documentos del expediente—.

Destacamos que no se han incluido en el cuadro siguiente los riesgos asociados a hechos o situaciones que, por su naturaleza, no tienen, *a priori*, un reflejo directo en el expediente ni, por lo tanto, son susceptibles de datificación, como sería el caso, paradigmáticamente, del pago de sobornos o de la filtración de informaciones sobre la contratación a potenciales operadores económicos interesados tanto en la fase de preparación como en la de licitación del contrato; o los incumplimientos o cumplimientos defectuosos de las prestaciones, cuya detección requiere verificaciones y comprobaciones materiales, y, por lo tanto, no generan *per se* datos en el expediente correspondiente.

Eso no significa que estos riesgos no sean detectables, pero no lo serán directa, sino indirectamente, a través de sus efectos o consecuencias en trámites del procedimiento o situaciones del ciclo de contratación que sí son susceptibles de datificación y, por lo tanto, de tratamiento por el sistema de alerta.

Con todos estos elementos, tenemos el cuadro siguiente:

Riesgo	Fase de contratación	Irregularidad	Alerta				Tipo	Nivel sistema alerta	Complejidad
			Definición	Datos					
				Identificación	Tipo	Personales			
Existencia de situaciones de conflicto de interés	Todas	Toma de decisión o actuación según criterios no imparciales ni objetivos como consecuencia de la interferencia de un interés particular en conflicto	Detección de vinculaciones entre servidores públicos que intervienen en el procedimiento de contratación y operadores económicos (participantes, licitadores y adjudicatarios)	Datos identificadores de los servidores públicos que participan directa o indirectamente (superiores jerárquicos o funcionales) en el procedimiento de contratación. Datos identificadores de los titulares reales / de las personas con cargos de responsabilidad en los operadores económicos participantes / licitadores	Procedimiento Otras bases de datos (organigramas / RM / titulares reales) Fuentes abiertas	Sí	Indiciaria	2	Media / Alta
Impulso o diseño de contrataciones innecesarias, sobredimensionadas, o perjudiciales	Preparación	Falta de justificación o justificación sesgada, inconsistente o incoherente de la contratación	Detección / comparación con contrataciones antecedentes con el mismo objeto Inexistencia de justifica-ción de la contratación Precios no de mercado	Justificación de la contratación Datos de contrataciones antecedentes Objeto contractual (pliegos) Tipo de licitación (pliegos) / precios de referencia de mercado	Procedimiento Contratación Otras bases de datos (precios de mercado)	No	Indiciaria	2	Media/ Alta
Elección indebida del procedimiento	Preparación	Utilización de procedimiento inadecuado / que elude o limita la competencia	Detección de inadecuación del procedimiento en función de las características del contrato	Tipo de procedimiento Justificación del procedimiento Tipo de licitación (pliegos) Objeto contractual (pliegos)	Procedimiento	No	Concluyente	0	Baja
Contrataciones con objetos inconcretos / mal definidos	Preparación	Falta de concreción suficiente del objeto contractual que facilita la arbitrariedad en la valoración de las ofertas	Detección de objeto contractual inconcreto / mal definido	Objeto contractual (pliegos)	Procedimiento	No	Indiciaria	0	Media
Limitación injustificada de la competencia en la licitación	Preparación	Diseño de requisitos de participación o de solvencia / criterios de selección cualita-tiva de participantes / licita-dores que limiten injustifica-damente la competencia	Detección de requisitos de participación o de solvencia / criterios de selección cualitativa injustificadamente restrictivos	Requisitos de participación o de solvencia / criterios de selección cualitativa de participantes / licitadores (pliegos)	Procedimiento	No	Concluyente Indiciaria	0	Baja / Media
Abuso de subcontratación (por diseño)	Preparación	Facilitar que el adjudicatario se convierta *de facto* en un poder adjudicador a través de la subcontratación Ocultar situaciones de conflicto de interés o de favoritismo a través de la subcontratación	Detección de exceso de subcontratación o subcontratación injustificadamente restrictiva en el diseño del contrato	Régimen de subcontratación (pliegos) Datos identificadores de los operadores económicos que hayan participado en actua-ciones preparatorias de la contratación Datos para la detección de situaciones de conflicto de interés (ver *supra*)	Procedimiento Contratación Otras bases de datos (RM / titulares reales)	Sí	Concluyente Indiciaria	2	Media / Alta
Intervención de licitador (adjudicatario) en el diseño de la contratación / en la elaboración de los pliegos	Preparación	Permitir la intervención directa de un licitador (previsiblemente adjudicatario del contrato) en el diseño de la contratación / la elaboración de los pliegos	Detectar intervenciones externas en los trabajos de preparación de la contratación	Pliegos y documentación del expediente de contratación (metadatos)	Procedimiento Otras bases de datos (organigramas / RM / titulares reales)	Sí	Indiciaria	2	Media

Riesgo	Fase de contratación	Irregularidad	Alerta				Tipo	Nivel sistema alerta	Complejidad
			Definición	Datos					
				Identificación	Tipo	Personales			
Criterios de valoración de ofertas inconcretos / mal definidos	Preparación	Diseño de criterios de valoración de les ofertes inconcretos / mal o poco definidos que faciliten la arbitrariedad en la valoración de las ofertas	Detección de criterios de valoración de las ofertas inconcretos / mal definidos	Criterios de valoración de ofertas y reglas / procedimientos para su aplicación (pliegos)	Procedimiento	No	Concluyente Indiciaria	0	Baja / Media
Fraccionamiento	Preparación / Adjudicación	Fraccionamiento del objeto contractual para eludir procedimientos con publicidad y concurrencia	Detección de acumulación en un mismo adjudicatario de múltiples contratos en un periodo corto de tiempo con objeto idéntico / análogo	Objeto contractual (pliegos) Adjudicatario Datos de contrataciones antecedentes	Procedimiento Contratación / contabilidad	Sí	Indiciaria	1	Baja
Asimetría de la información en la licitación	Licitación	Creación de déficits o asimetrías en la información facilitada a los participantes / licitadores	Detección de anomalías en la puesta a disposición de los operadores económicos interesados de la información de la licitación	Publicaciones de la licitación	Procedimiento	No	Indiciaria	0	Baja / Media
Incumplimiento de los plazos mínimos de licitación	Licitación	Falseamiento de la libre concurrencia reduciendo indebidamente el plazo para la presentación de ofertas	Detección de plazo de presentación de ofertas indebidamente breve	Plazo de presentación de ofertas (pliegos / publicaciones de la licitación)	Procedimiento	No	Concluyente Indiciaria	0	Baja
Prácticas colusorias	Licitación	Falseamiento de la libre concurrencia mediante colusión entre los licitadores (con o sin conocimiento / consentimiento del ente contratante)	Detección de prácticas colusorias a través de múltiples indicadores, entre otros: - licitador único; - única oferta admisible; - reiteración de los mismos licitadores con estructuras de ofertas análogas / adjudicaciones rotatorias; - estructura anormal de bajas; - presentación de ofertas por operadores vinculados	Datos identificadores de los participantes / licitadores y de los titulares reales / de las personas con cargos de responsabilidad en los operadores económicos participantes / licitadores Características de las ofertas (bajas / otros elementos de las ofertas) Participantes / licitadores inadmitidos	Procedimiento Contratación Otras bases de datos (RM / titulares reales)	Sí	Indiciaria	2	Alta
Admisión o exclusión indebida de participantes / licitadores	Licitación	Admisión o exclusión indebida de participantes / licitadores que comporte alteración del principio de igualdad de trato y falsee la competencia	Detección de admisiones o exclusiones irregulares de participantes / licitadores	Requisitos de solvencia / criterios de selección cualitativa de participantes / licitadores y régimen de ofertas anormales (pliegos) Aplicación de los criterios de selección cualitativa de participantes / licitadores (informes del procedimiento) Inadmisión de ofertas (informes de la licitación) Aplicación irregular del régimen de ofertas anormales (informes de la licitación)	Procedimiento	No	Concluyente Indiciaria	0	Media

Riesgo	Fase de contratación	Irregularidad	Alerta				Tipo	Nivel sistema alerta	Complejidad
			Definición	Datos					
				Identificación	Tipo	Personales			
Valoración irregular / sesgada de las ofertas	Adjudicación	Aplicar irregularmente / sesgadamente o modificar los criterios de valoración de las ofertas de forma que se favorezca y/o perjudique determinados licitadores	Detección de irregularidades en la aplicación de los criterios de valoración de ofertas	Criterios de valoración de ofertas y reglas / procedimientos para su aplicación (pliegos) Aplicación de los criterios de valoración de ofertas (informes de la licitación / de adjudicación) Existencia / composición del comité de expertos cuando sea preceptivo (art. 146.2 a) LCSP: criterios dependiente de un juicio de valor con ponderación superior a criterios automáticos) Datos identificadores de los integrantes del comité de expertos cuando sea preceptivo	Procedimiento Otras bases de datos	Sí	Concluyente Indiciaria	2	Media / Alta
Adjudicación a licitador que no ha presentado la mejor oferta	Adjudicación	Adjudicar el contrato a un licitador que no es el que ha presentado la mejor oferta Apartarse injustificadamente de la propuesta de adjudicación de la mesa de contratación	Detección de adjudicación a licitador diferente del propuesto / del que ha obtenido la mejor puntuación	Aplicación de los criterios de valoración de ofertas (informes de la licitación / de adjudicación) Propuesta de adjudicación Resolución de adjudicación	Procedimiento	No	Concluyente Indiciaria	0	Baja / Media
Irregularidades en los recursos	Licitación / Adjudicación	No tramitar / no resolver / resolver irregularmente los recursos que puedan presentar los participantes / licitadores	Detección de recursos no tramitados / no resueltos / irregularmente resueltos	Recursos presentados Recursos resueltos Sentido / motivación / racionalidad de la resolución	Procedimiento	No	Concluyente	0	Media / Alta
Desistimiento injustificado del procedimiento de contratación	Licitación / Adjudicación	Desistir injustificadamente del procedimiento de contratación	Detección de desistimiento injustificado del procedimiento de contratación	Resolución de desistimiento del procedimiento de contratación: motivación / racionalidad	Procedimiento	No	Concluyente Indiciaria	0	Media
Irregularidades en la formalización del contrato	Adjudicación	Formalización del contrato fuera de los plazos establecidos / con modificaciones respecto de las previsiones de los pliegos / con condiciones no previstas / etc.	Detección de formalización en fecha anormal Detección de discordancias entre el documento de formalización y las previsiones de los pliegos	Fecha de formalización Documento de formalización Pliegos	Procedimiento	No	Concluyente Indiciaria	0	Media
Incumplimientos de plazos contractuales	Ejecución	Incumplimiento por parte del contratista de los plazos parciales o total para la ejecución del contrato	Detección de superación de plazos parciales o total del contrato sin que conste la ejecución de las prestaciones contratadas	Plazos contractuales, parciales o total (pliegos) Documentación de ejecución (informes / facturas conformadas)	Procedimiento	No	Indiciaria	0	Baja
Incrementos de precios irregulares o no justificados	Ejecución	Aceptar revisiones de precios o precios contradictorios irregulares, no justificados o excesivos	Detección / comparación con contrataciones antecedentes con el mismo objeto Inexistencia de justificación de la revisión de precios / precios contradictorios Precios no de mercado	Justificación de la revisión de precios / precios contradictorios (pliegos / informes de ejecución) Datos de contrataciones antecedentes Precios de referencia de mercado	Procedimiento Contratación Otras bases de datos (precios de mercado)	No	Indiciaria	2	Media / Alta

Riesgo	Fase de contratación	Irregularidad	Alerta				Tipo	Nivel sistema alerta	Complejidad
			Definición	Datos					
				Identificación	Tipo	Personales			
Modificaciones irregulares del contrato	Ejecución	Modificación del contrato fuera de los supuestos legalmente admitidos, que alteren su contenido o elementos esenciales del mismo o que habrían permitido la adjudicación a otros participantes / licitadores	Detección de modificaciones que incumplen las limitaciones cuantitativas (prestaciones / precio), cualitativas (previsiones en los pliegos) o temporales legal o contractualmente establecidas	Justificación de las modificaciones (informes de ejecución) Características de las modificaciones Resoluciones de modificación	Procedimiento	No	Concluyente Indiciaria	0	Media
Continuidad irregular de la ejecución de contratos con plazo de ejecución vencido	Ejecución	Continuar fuera de los supuestos legalmente admitidos la ejecución por vía de hecho (prestaciones y pago) de un contrate cuyo plazo ha finalizado	Detección de la ejecución de prestaciones más allá de la fecha de finalización del contrato	Fecha de finalización Documentación de ejecución (informes / facturas / etc.)	Procedimiento	No	Concluyente Indiciaria	0	Baja / Media
Adjudicación sin publicidad ni concurrencia de contratos complementarios	Adjudicación / Ejecución	Adjudicar al adjudicatario de un contrato otros contratos complementarios fuera de los casos legalmente admitidos	Detección de la adjudicación de contratos complementarios	Resoluciones de adjudicación de contratos complementarios Datos identificadores del adjudicatario Justificación de los contratos complementarios	Procedimiento Contratación	Sí	Indiciaria	1	Media
Pagos indebidos	Ejecución	Aprobar pagos indebidos (adelantos indebidos; pagos duplicados; facturación de prestaciones no ejecutadas / no claramente identificadas / indebidas; etc.)	Detección de incoherencias / contradicciones entre las facturas presentadas y pagos acordados y las previsiones económicas del contrato	Documentación y datos de ejecución (informes / facturas) Resoluciones de aprobación de facturas y pagos Datos económicos del contrato (pliegos / adjudicación / formalización)	Procedimiento	No	Concluyente	0	Baja
Abuso de subcontratación (en ejecución)	Licitación / Ejecución	Irregularidades en la subcontratación: - subcontratación que exceda de los límites establecidos / no informada en la litación / no permitida; - subcontratación de licitadores no adjudicatarios u operadores que han participado en la preparación de la contratación	Detección: - de excesos de subcontratación / de subcontratación no admisible; - de subcontratación de licitadores no adjudicatarios o de operadores que han participado en actuaciones preparatorias de la contratación	Documentación y datos de ejecución (subcontratación) Datos identificadores del/de los subcontratista/s (constancia en principio en la oferta)	Procedimiento Contratación	Sí	Concluyente Indiciaria	1	Media
Subrogación irregular del contratista	Ejecución	Aprobar la subrogación de otro operador en la posición del contratista cuando no lo permiten los pliegos o el régimen legal o ello comporte la alteración sobrevenida de los requisitos de solvencia / criterios de selección cualitativa de participantes / licitadores	Detección de subrogación de otros operadores en la posición del contratista / características del subrogado	Documentación y datos de ejecución (subrogación) Datos identificadores del subrogado Régimen de subrogación (pliegos) Requisitos de solvencia / criterios de selección cualitativa de participantes / licitadores (pliegos)	Procedimiento	Sí	Concluyente Indiciaria	0	Media / Alta

5 Conclusiones y recomendaciones

5.1 Conclusiones

De acuerdo con cuanto se ha expuesto hasta este punto, pueden formularse las conclusiones siguientes:

Primera. Los **sistemas automatizados de alerta** son un **elemento esencial en cualquier sistema de integridad**. Es previsible —y, en todo caso, sería altamente deseable— que este tipo de sistemas tengan un desarrollo y crecimiento muy relevante en los próximos años en la medida en que se ha demostrado que constituyen una de las herramientas más potentes y eficaces en la prevención, detección, corrección y persecución de irregularidades y de situaciones de fraude y de corrupción.

El estado de situación actual, tanto en la Generalitat de Cataluña como en el ámbito local, no permite ser optimista. Se constata que, a pesar de los grandes avances llevados a cabo en la digitalización del sector público y, concretamente, en la implementación de soluciones para la tramitación electrónica de los procedimientos de contratación, el desarrollo de sistemas automatizados de alerta no parece una prioridad y sólo se ha concretado en casos ultraminoritarios.

Se constata pues **un déficit significativo** en el sector público catalán a la hora de sacar provecho y **explotar todas las potencialidades de la datificación de la contratación pública al servicio de la integridad**. El mandato general de servicio con objetividad de los intereses generales, que obliga a todos los poderes públicos y que implica que toda su actividad se encuentre sometida al principio de integridad, tendría que comportar la adopción de todas las medidas necesarias para reconducir esta situación los próximos años.

Segunda. El contexto actual presenta factores muy favorables al desarrollo y la implantación efectiva de sistemas automatizados de alerta en tanto que:

a. se constata una extensión de la datificación de la actividad del sector público a medida que se generaliza la implantación de soluciones técnicas para la tramitación electrónica de los procedimientos especialmente en el ámbito de la contracción pública; y

b. los fondos NextGenerationEU aportarán previsiblemente un gran volumen de recursos económicos para el desarrollo de proyectos en el ámbito que nos ocupa y, además, imponen unos requisitos y exigencias de integridad que tendrían que generalizarse a toda la contestación pública —y no sólo en aquella parte financiada con fondo europeos— y perpetuarse más allá de la finalización de aquel programa europeo, convirtiéndose en un elemento estructural de nuestro marco legal y de gestión de la contratación pública.

Tercera. Todos los desarrollos digitales y proyectos del sector público que, aprovechando aquella ventana de oportunidad, contribuyan al desarrollo de la digitalización del sector público y de su actividad tendrían que incorporar el **principio de i*ntegridad por diseño*** en su concepción e implementación y, por lo tanto, incorporar mecanismos de detección y prevención de riesgos para la integridad, no como una opción complementaria sino como un elemento integrante de la estructura principal vertebradora de toda solución tecnológica, especialmente en el ámbito de la contratación pública.

Cuarta. No existe un único sistema de alerta aplicable a cualquier organización o entidad contratante. En este ámbito el contexto lo es todo y, por lo tanto, el primer paso metodológico será la **identificación de las alertas relevantes y útiles**, de todas las posibles, teniendo en cuenta las especificidades de la organización donde se pretenda implementar el sistema de alerta y del marco legal y operativo existente.

Este primer paso consiste en el **proceso de identificación, análisis y evaluación de los riesgos** que constituye el objeto de una parte importante de los materiales del proyecto *Riesgos para la integridad en la contratación pública* de la Oficina Antifraude y, por lo tanto, muchos los documentos y herramientas producidos en el marco de aquel proyecto son de gran utilidad en esta fase inicial del diseño de un sistema de alertas.

Quinta. La **disponibilidad y calidad de los datos** de que se nutren los sistemas de alerta constituyen un elemento clave de su eficacia. Desde este punto de vista, la **superioridad de los sistemas internos** es indiscutible.

Hace falta pues centrar los esfuerzos en el desarrollo de sistemas de alerta de carácter interno, que se nutran de datos directamente obtenidos de los gestores electrónicos de expedientes y se diseñen con capacidad para interactuar automatizadamente con éstos para garantizar el efecto realmente preventivo de las alertas.

Sexta. Por otra parte no hay que olvidar que los sistemas de alerta son ante todo herramientas al servicio de las instancias de control interno, sin perjuicio de su igualmente innegable utilidad para los órganos de control externo e incluso al servicio de la transparencia y de la rendición de cuentas.

La participación de los órganos de control interno en el diseño e implementación de los sistemas de alerta es pues necesaria y esencial.

Séptima. La potencia y eficacia de un sistema de alertas viene determinada en gran medida por la cantidad y calidad de las fuentes de datos que utilice. En este sentido los referentes más avanzados en el ámbito que nos ocupa, la herramienta Arachne de la Comisión Europea y el sistema SALER de la Comunidad Valenciana utilizan datos de tres grandes categorías de fuentes:

a. datos del gestor electrónico de expedientes de contratación, referidos al procedimiento concreto que se está tramitando;

b. datos de contratación y de contabilidad del ente contratante; y

c. datos adicionales de carácter externo, tanto de registros o bases de datos públicos, como, con las debidas cautelas y garantías en materia de protección de datos personales, datos abiertos de Internet.

Octava. El respeto de las limitaciones y garantías derivadas del marco legal europeo y nacional en materia de protección de datos personales constituye un elemento clave que no puede ser descuidado en el diseño e implementación de cualquier sistema de alerta basado en datos.

Se detecta la necesidad de mejorar las previsiones y disposiciones del marco legal nacional para dar cobertura a sistemas de alertas más potentes y eficaces.

Novena. Diseñar e implementar un sistema de alerta sin prever los **recursos materiales, personales y operativos necesarios para gestionar, verificar y hacer el seguimiento de las alertas generadas** y aprovechar al máximo todas las potencialidades de un sistema de este tipo es un despilfarro de recursos públicos.

Un sistema automatizado de alertas es un instrumento al servicio de la integridad, y la medida de su utilidad es su efectividad. Por lo tanto, tan importante como disponer de un sistema de alertas es definir claramente el tratamiento y efectos de las alertas que genere y garantizar la adscripción de los recursos adecuados para asegurar la efectividad real de todas sus potencialidades.

5.2 Recomendaciones y consideraciones

Teniendo en cuenta estas conclusiones generales del presente estudio, y de conformidad con lo que dispone el art. 3 c) de la Ley 14/2008, de 5 de noviembre, de la Oficina Antifraude de Cataluña, se considera procedente la formulación de las siguientes recomendaciones y consideraciones.

5.2.1 Al Departamento de Economía y Hacienda de la Generalitat de Cataluña, y, específicamente, a la Dirección General de Contratación Pública y a la Intervención General; y al Departamento de la Vicepresidencia y de Políticas Digitales y Territorio

Primera. La Administración de la Generalitat de Cataluña y todos los entes instrumentales que integran su sector público tienen que profundizar y avanzar en la digitalización y la datificación de su actividad, aprovechando especialmente los recursos y los imperativos de integridad de los fondos NextGenerationEU, y dotarse de sistemas automatizados de alerta basados en la explotación y análisis de datos.

En este sentido, sería deseable diseñar, desarrollar e implantar en el GEEC 2.0 y, si procede, en el TEEC este tipo de sistema de alerta, además de generalizar el uso del GEEC y del TEEC en todo el sector público de la Generalitat.

El diseño, desarrollo e implantación en el GEEC y el TEEC de sistemas automatizados de alerta tendría que llevarse a cabo con la participación de la

Intervención General y del CTTI y, con la colaboración de la Sindicatura de Cuentas y de la Oficina Antifraude.

Segunda. El uso de datos personales por los sistemas automatizados de alerta tiene que ser plenamente compatible y conforme con el marco legal vigente europeo y nacional en materia de protección de datos.

En este sentido, sería deseable estudiar y, en la medida en que sea necesario, llevar a cabo las modificaciones y adaptaciones normativas adecuadas con el fin de garantizar que el tratamiento de datos personales para garantizar la integridad en la contratación pública tenga la condición de tratamiento por obligación legal, interés público o ejercicio de poderes públicos, de acuerdo con aquello que disponen el art. 8 de la LOPDGDD y el art. 6 del RGPD.

Tercera. En cualquier caso, y con carácter general, cualquier desarrollo tecnológico de la Generalitat de Cataluña y del CTTI debería regirse por el **principio de i*ntegridad por diseño*** en su concepción e implementación y, por lo tanto, incorporar mecanismos de detección y prevención de riesgos para la integridad como un elemento integrante de la estructura principal vertebradora de toda solución tecnológica, especialmente en el ámbito de la contratación pública.

5.2.2 Al Consorcio Localret

Cuarta. El Consorcio Localret ha iniciado el procedimiento para la conclusión de un acuerdo marco para la adquisición de una solución informática para el seguimiento, control y planificación de los contratos públicos de los entes locales, según los resultados de la consulta preliminar de mercado previamente llevada a cabo.

Reconociendo el gran valor y utilidad para todos los entes locales de esta iniciativa, sería deseable que en el procedimiento de negociación para la conclusión de aquel acuerdo marco y en el subsiguiente proceso de desarrollo de aquella herramienta se contemplara la incorporación como elemento esencial las principales funcionalidades correspondiendo a un sistema de alertas para la integridad en las diversas fases del ciclo de contratación pública.

Quinta. Asimismo, y con carácter general, se recomienda al Consorcio Localret que cualquier desarrollo tecnológico que pueda impulsar en el futuro se rija por el mencionado **principio de i*ntegridad por diseño*** en su concepción e implementación.

5.2.3 Al Consorcio AOC, a los entes locales beneficiarios de fondos del PRTR, a las Diputaciones Provinciales, a los Consejos Comarcales y al Área Metropolitana de Barcelona, a través de su Agencia de Transparencia

Sexta. Debe aprovecharse el impulso a los procesos de digitalización y datificación de la actividad del sector público local que suponen los programas específicos con esta finalidad del PRTR financiado con los fondos

NextGenerationEU para incorporar sistemas automatizados de alerta basados en la explotación y análisis de datos, concebidos, en primera instancia —aunque evidentemente con un alcance más amplio—, como herramientas al servicio de las instancias de control interno.

Séptima. Asimismo, y con carácter general, se recomienda igualmente que cualquier desarrollo tecnológico que se pueda llevar a cabo o impulsar por las entidades destinatarias de estas recomendaciones se rija por el mencionado **principio de i*ntegridad por diseño*** en su concepción e implementación.

5.2.4 Al Colegio de Registradores de la Propiedad y Mercantiles de España

Octava. Los datos organizativos —identificación de las personas representantes o titulares de cargos de gestión y administración— y de titularidad de las empresas participantes en los procesos de contratación pública son datos clave de enorme utilidad para la implementación de numerosas alertas automatizadas en el ámbito que nos ocupa. Sería por lo tanto deseable facilitar el acceso automatizado a los mismos.

Se somete pues a la consideración del Colegio de Registradores de la Propiedad y Mercantiles de España la conveniencia de estudiar las posibilidades de facilitar el acceso automatizado a los datos del Registro Mercantil y de Titularidades Reales a los sistemas de alertas que puedan diseñar e implementar las entidades del sector público.