Oficina Antifrau
de Catalunya

Sistemes automatitzats d'alerta en l'àmbit de la contractació pública

Estudi

L'Oficina Antifrau és una institució independent, adscrita al Parlament de Catalunya, encarregada de prevenir i investigar la corrupció així com de preservar la transparència i la integritat de les administracions i del personal al servei del sector públic a Catalunya.

Al novembre de 2020 la Direcció va aprovar la *Memòria inicial de l'estratègia d'intel·ligència basada en anàlisi de dades de l'Oficina Antifrau de Catalunya*, amb l'objectiu de dotar-se d'una estratègia pròpia en l'àmbit de la intel·ligència basada en l'anàlisi de dades (*data-driven intelligence*), al servei de la missió i les funcions de l'Oficina. L'horitzó temporal inicial d'aquesta iniciativa és de tres anys, 2021 a 2023, i per al seu desenvolupament s'ha constituït un grup de treball dedicat, l'Equip d'Anàlisi de Dades.

Aquest estudi és el primer producte d'aquella estratègia, corresponent al primer dels projectes que l'integren, desenvolupat al llarg de l'any 2021. El seu objectiu és determinar l'estat de situació, estudiar els referents existents i formular algunes orientacions i recomanacions per tal de fomentar el disseny i implementació de sistemes automatitzats d'alerta en l'àmbit de la contractació pública.

Oficina Antifrau de Catalunya | Equip d'Anàlisi de Dades
Autor: Bruno González Valdelièvre

Reconeixement – no comercial – sense obra derivada:
no es permet un ús comercial de l'obra original ni la generació d'obres derivades

Setembre de 2022 (versió revisada i actualitzada)

www.antifrau.cat | bustiaoac@antifrau.cat

Oficina Antifrau de Catalunya

Equip d'Anàlisi de Dades

Sistemes automatitzats d'alerta en l'àmbit de la contractació pública

Índex

0 **Resum executiu** 3

1 **Introducció i consideracions prèvies** 6

1.1 Introducció 6

1.2 Sobre el contingut d'aquest document 7

1.3 Concepte 8

2 **Diagnosi** 10

2.1 Context general 10

2.1.1 *Marc normatiu: procediment electrònic i contractació electrònica* 10

2.1.2 *Nous paradigmes: transparència i dades obertes* 16

2.1.3 *Marc conceptual: la datificació al servei de la integritat* 19

2.2 El cigne negre: fons NextGenerationEU 22

2.2.1 *Recursos* 23

2.2.2 *Requisits d'integritat* 24

2.3 Situació 27

2.3.1 *Generalitat de Catalunya* 27

2.3.2 *Àmbit local* 31

2.3.3 *Perspectives* 35

3 **Referents** 39

3.1 Eina Arachne 39

3.1.1 *Dades internes* 41

3.1.2 *Dades externes* 41

3.1.3 *Indicadors generats per Arachne* 42
3.2 Sistema SALER 44
3.3 Document *Red Flags for Integrity* (OCP, 2016-2021) 49
3.3.1 *Interès i utilitat dels sistemes d'alerta* 50
3.3.2 *Idees clau* 51
3.3.3 *Metodologia* 52
4 Anàlisi 58
4.1 Prevenció i contingència 58
4.2 Sistemes externs vs. interns 61
4.3 Tipologia: 3 nivells de sistemes d'alerta 63
4.3.1 *Nivell 0: el gestor electrònic d'expedients* 64
4.3.2 *Nivell 1: explotació de les dades de contractació i comptabilitat* 65
4.3.3 *Nivell 2: creuament amb d'altres dades internes i externes* 66
4.4 Metodologia: del mapa de riscos als elements d'un sistema d'alerta 68
5 Conclusions i recomanacions 76
5.1 Conclusions 76
5.3 Recomanacions i consideracions 78

0 Resum executiu

Aquest estudi tracta dels **sistemes automatitzats d'alerta en l'àmbit de la contractació pública**, definits com a sistemes tecnològics que, processen mitjançant els corresponents algoritmes dades de diverses fonts, tant intrínseques als procediments de contractació com extrínseques als mateixos, detecten i posen automatitzadament en coneixement de les instàncies de control, internes i/o externes, l'existència o la possibilitat —i, eventualment, en aquests casos, la probabilitat— d'irregularitats i, en el seu cas, n'impedeixen l'efectiva materialització.

L'interès i l'oportunitat d'aquest estudi es justifiquen per la coincidència d'una sèrie de tendències estructurals i, alhora, d'una circumstància conjuntural que, en convergir en el moment actual, generen **una finestra d'oportunitat** en aquesta vessant de la lluita contra el frau i la corrupció, que hauria de ser aprofitada per totes les instàncies i institucions amb un compromís ferm amb la integritat en la gestió pública.

Les **grans tendències de fons** que afavoreixen el desenvolupament dels sistemes d'alerta d'aquesta naturalesa són, en primer lloc, el desenvolupament d'un **marc legal** que impulsa i, en certa mesura, imposa la tramitació electrònica dels procediments administratius, especialment dels procediments de contractació; aquest marc legal ja ha assolit una certa maduresa especialment a Catalunya, amb la promulgació del Decret 76/2021, de 4 d'agost, d'Administració digital.

En segon lloc, també tenen una indubtable rellevància la **consolidació dels paradigmes de la transparència i les dades obertes**, que s'han anat implantant, normativament i operativa, en l'última dècada.

Aquestes tendències han donat lloc al desenvolupament i la progressiva implementació en els diversos nivells del sector públic —local, autonòmic i estatal— de solucions tecnològiques per a la tramitació íntegrament electrònica dels procediments, donant lloc al fenomen de la ***datificació* de l'activitat del sector públic**. És a dir, la generació per la pròpia tramitació administrativa de dades en suports electrònics susceptibles de ser recopilades, emmagatzemades, tractades i explotades amb múltiples finalitats i, entre elles, i als efectes que aquí ens interessen, al servei de la integritat, per a la prevenció, detecció, correcció i persecució d'irregularitats i de supòsits de frau o de corrupció.

La **circumstància conjuntural favorable** és la creació per part de les institucions de la Unió Europea de l'**instrument temporal de recuperació NextGenerationEU** que, a través del Pla de Recuperació, Transformació i Resiliència aprovat per la Comissió Europea, hauria d'accelerar i fomentar el desenvolupament d'aquelles tendències.

Per una banda, l'instrument NextGenerationEU aporta un ingent volum de recursos destinats al desenvolupament i la transformació digital del sector públic.

Per altra banda, la normativa europea reguladora d'aquell instrument imposa als gestors i beneficiaris dels recursos corresponents unes obligacions d'integritat especialment intenses —que, tot sigui dit, haurien de generalitzar-se a tota la contractació pública i no exclusivament a aquella finançada amb fons europeus—.

L'estudi s'estructura en quatre grans parts.

En la **primera part** s'estudien en detall els **elements contextuals**, estructurals i conjunturals, que acabem d'apuntar, i s'analitza l'**estat de situació**, tant en l'administració autonòmica catalana com en l'àmbit local, el que ens porta a una constatació: si bé la contractació electrònica ha assolit un grau d'implantació rellevant tant en l'administració de la Generalitat com en els ens locals —com a mínim en els de més entitat que disposen de més recursos—, la implementació de sistemes automatitzats d'alerta és a hores d'ara absolutament minoritària i excepcional.

En aquest context, s'estudia una iniciativa de gran interès del Consorci Localret, actualment en curs, destinada a dotar els ens locals d'una eina tecnològica de seguiment, control i planificació de la contractació.

La **segona part** de l'estudi analitza en detall **tres grans referents** d'enorme interès: l'**eina Arachne**, solució tecnològica basada en dades de referència de la Comissió Europea, que aquesta posa a disposició de tota organització o entitat gestora de fons europeus com a eina de lluita antifrau; el **sistema SALER** de la Comunitat Valenciana, pioner en l'àmbit que ens ocupa; i el **document *Red Flags for Integrity***, referència conceptual, metodològica i pràctica inexcusable per al disseny i implementació de sistemes d'alerta.

En la **tercera part**, es desenvolupen una sèrie de reflexions i consideracions sobre els sistemes automatitzats d'alerta, que incideixen en la **capacitat preventiva** —més enllà de la seva utilitat contingent— en la mesura en que poden permetre la detecció en temps real de possibles o potencials irregularitats, fraus i supòsits de corrupció, evitant per tant que s'arribin a materialitzar.

A continuació es considera la distinció entre **sistemes d'alerta interns**, que exploten les dades directament obtingudes del gestor electrònic d'expedients, i **sistemes externs**, que obtenen les dades d'altres fonts —registres, portals o plataformes de contractació—, el que ens portarà a la conclusió de la superioritat dels primers. Així mateix es destaca com els sistemes d'alerta s'han de concebre primàriament i prioritària com una eina al servei de les instàncies de control intern, sens perjudici d'altres importants potencialitats i utilitats que puguin tenir.

En tercer lloc es defineix una **tipologia de sistemes d'alerta**, basada en les diverses categories de dades de que es nodreixen —dades exclusivament del procediment de contractació que es tramita; del conjunt de la contractació i de la comptabilitat de l'entitat de que es tracti; o dades anteriors enriquides amb dades d'altres bases de dades i fonts externes— el que determina la menor o major capacitat de detecció d'irregularitats, fraus i corrupció.

I finalment, aquesta tercera part conclou amb un intent de recapitular els **elements metodològics** apuntats en aquest estudi, i intenta oferir una síntesi dels elements bàsics i aspectes principals a tenir en compte. A títol il·lustratiu, s'inclou un quadre on s'ha procurat definir els elements essencials de les diverses alertes corresponents als principals riscos en el cicle de la contractació pública.

La quarta i última part de l'estudi conté les **conclusions** de tot el que s'ha exposat i una sèrie de **recomanacions** adreçades a diversos poders públics i institucions.

1 Introducció i consideracions prèvies

1.1 Introducció

L'any 2017 la Direcció de Prevenció de l'Oficina Antifrau va iniciar el projecte *Riscos per a la integritat en la contractació pública*. En el marc d'aquest projecte, que culmina enguany amb la publicació, al gener de 2021, de l'informe final titulat *Compra pública: una cartografia dels riscos inherents i dels factors on enfocar la prevenció*, i amb la propera formulació d'una sèrie de recomanacions preventives adreçades als poders públics i als òrgans de contractació, s'han generat una sèrie de documents i eines de gran valor[1], reconegut a nivell nacional i internacional; entre d'altres:

a. 8 documents tècnics de treball adreçats principalment a les persones intervinents en els procediments de contractació;

b. una guia interactiva orientada a facilitar l'anàlisi de riscos en les diverses organitzacions públiques destinatàries; i

c. diverses eines i recursos de suport a la prevenció en aquest àmbit, així com les aportacions de persones expertes que van analitzar, des de diferents perspectives, els riscos per a la integritat en la contractació pública.

Les actuacions dutes a terme per l'Oficina Antifrau en el marc d'aquell projecte han consistit, en síntesi, en un exhaustiu i profund estudi qualitatiu de la contractació pública a Catalunya —tal i com s'indica en la pàgina de presentació del projecte al web de l'Oficina—.

El present document pretén donar continuïtat i alhora complementar aquell estudi qualitatiu des d'una perspectiva diferent: la perspectiva quantitativa i tecnològica. Ens proposem aquí posar el focus de la nostra anàlisi i reflexió en els **sistemes automatitzats d'alerta en l'àmbit de la contractació pública**.

Com veurem tot seguit, la pertinència i oportunitat d'aquest estudi es justifiquen per diverses circumstàncies que convergeixen en el moment actual, que dona lloc a una interessant finestra d'oportunitat:

a. d'una banda, com a grans tendències de fons, cal fer esment, en primer lloc, a la implantació, cada vegada més estesa i profunda, de solucions informàtiques per a la tramitació íntegrament electrònica dels procediments de contractació pública —el que respon a un imperatiu normatiu tant europeu com nacional—; així mateix, i paral·lelament, s'observa el progressiu desenvolupament i implantació d'una cultura i d'una governança de les dades, especialment visible i rellevant en l'àmbit de la contractació pública, impulsades i fomentades per la implantació legal i operativa dels paradigmes de la transparència i les dades obertes; i,

[1] Tots els documents i materials es poden accedir, consultar i descarregar des de la pàgina de presentació del projecte al web de l'Oficina Antifrau: https://www.antifrau.cat/ca/prevencio/arees-d-estudi/contractacio-publica

igualment, en aquest context, cal destacar l'aparició, els últims anys, d'estudis i propostes i també de projectes concrets, cada vegada més nombrosos, de desenvolupament i implantació de sistemes automatitzats d'alerta basats en l'anàlisi de dades;

b. d'altra banda no podem ignorar un factor accelerador i impulsor conjuntural i específic d'aquest moment —finals de 2021—: el previsible impuls decisiu a la transformació digital de tot el sector públic que haurien de suposar els fons provinents de l'instrument NextGeneration EU.

1.2 Sobre el contingut d'aquest document

Aquest estudi no pretén determinar, de manera unívoca i tancada, com ha de ser i com s'ha de configurar un sistema automatitzat d'alerta.

La raó sembla evident: no existeix una solució única; no existeix —ni probablement existirà— una aplicació informàtica en un llapis de memòria que, instal·lada en els servidors d'un ens públic, garanteixi la integritat, la conformitat a Dret, la gestió òptima i la plena correcció de la contractació pública.

Com veurem, les possibilitats i les diverses opcions són gairebé infinites i la determinació de la solució més adient en cada cas requereix una prèvia anàlisi i avaluació tant del context normatiu i operatiu com dels riscos realment existents, que poden ser molt diferents en les diverses organitzacions concernides.

Així doncs, el que pretenem aquí es, en primer lloc, realitzar una diagnosi de l'estat de situació en l'àmbit considerat; d'altre banda, pretenem plantejar una sèrie de reflexions i consideracions, tant a nivell conceptual com des del punt de vista metodològic i més operatiu, amb l'objectiu de fomentar la presa de consciència per tots els poders públics de la importància estratègica de desenvolupar i implementar aquest tipus de sistemes d'alerta; finalment, i en aquesta línia, es formulen diverses recomanacions adreçades als poders públics —i també als operadors privats— per aprofitar i desenvolupar al màxim les potencialitats del context i del moment concret en el qual ens trobem.

Aquest estudi es concep doncs, més que com el resultat final, definitiu i tancat, d'un estudi sectorial, com un punt de partida, obert i impulsor —també voldríem que inspirador— de futurs desenvolupaments, absolutament necessaris.

El document s'estructura en els apartats següents:

a. **diagnosi**: anàlisi del context general —tant pel que fa a les grans tendències estructurals com als factors conjunturals— i de la situació actual en l'àmbit que ens ocupa, tant a nivell local com autonòmic català;

b. **referents**: breu repàs i descripció d'alguns referents més propers i d'especial interès;

c. **anàlisi**: reflexions i consideracions conceptuals, metodològiques i operacionals; i

d. **conclusions**: recapitulació i formulació de propostes i recomanacions.

1.3 Concepte

L'expressió sistema d'alerta és polisèmica i ambigua. Pot referir-se —i, de fet, en diversos documents i contextos, es refereix efectivament— a realitats bastant diferents:

a. en alguns casos fa referència a projectes d'anàlisi de dades de contractació, basats en dades obertes o en dades extretes de plataformes de contractació, a partir de les quals es generen indicadors de risc: aquest seria el cas, per exemple, d'Opentender, plataforma de dades de contractació pública del projecte DIGIWHIST[2]; o del projecte hongarès Red Flags[3];

b. també se solen designar com a *sistemes d'alerta* determinats sistemes basats en l'ús de dades massives que ofereixen en temps real —en major o menor mesura— informació per a la detecció d'irregularitats i per a l'avaluació de riscos: un exemple plenament operatiu seria l'eina Arachne, creada i gestionada per la Comissió Europea[4]; igualment el sistema SALER de la Inspecció General de Serveis de la Generalitat Valenciana, tal i com apareix descrit en la seva norma de creació[5], s'inclouria en aquesta categoria;

c. però un sistema d'alerta també és, indubtablement, un canal de comunicació segur per a alertadors.

---

[2] El projecte *DIGIWHIST, The Digital Whistleblower* —digiwhist.eu—, és un projecte de recerca finançat per la Unió Europea (EU) que es va dur a terme entre 2015 i 2018, amb la participació de 6 universitats i institucions de recerca del Regne Unit, Alemanya, Hongria, la República Txeca i Itàlia. Un dels productes del projecte és la plataforma Opentender —opentender.eu— que recopila dades de licitacions de 33 jurisdiccions —els 28 estats membres de la UE, les institucions europees, Noruega, Islàndia, Suïssa i Geòrgia— dels anys 2009 a 2020 i ofereix diversos indicadors —6 indicadors de capacitat administrativa, 10 de transparència i 7 d'integritat—. Les dates utilitzades provenen de diverses fonts però principalment de la plataforma de contractació de la Unió Europea TED (*Tenders Electronic Daily*);

[3] El projecte *Red Flags (Prevention and detection of corrupt procurements through analysis, red flags and follow up*) —www.redflags.eu—, és igualment un projecte finançat per la UE en el qual van participar Transparència Internacional (TI) Hongria, la ONG hongaresa K-Monitor i PetaByte. Centrat en les dades de contractació hongareses, la web del projecte aplica, a cadascun dels anuncis de licitació i d'adjudicació publicats des de 2012 uns indicadors —31 indicadors per als anuncis de licitació i 9 pels anuncis d'adjudicació— generadors d'alertes indicatives de riscos en la contractació corresponent.

[4] D'acord amb la presentació i el dossier informatiu publicats per la Comissió Europea —cfr. nota 49 *infra*—, Arachne és una eina tecnològica de mineria de dades desenvolupada per la Comissió des de 2009 i plenament operacional des de setembre de 2015, posada a disposició dels diversos estats membres de la UE com a eina per a la prevenció d'irregularitats, frau i corrupció en la gestió de fons europeus. Com veurem més endavant, l'eina fa servir dades internes, facilitades pels propis ens gestors i de control dels fons europeus, i externes, facilitades per dos proveïdors externs, Orbis i World Compliance, i ofereix fins a 106 indicadors de risc classificats en 7 categories. L'eina Arachne serà objecte d'anàlisi detallat en l'apartat 3.1 del present estudi.

[5] La Llei valenciana 22/2018, de 6 de novembre, d'Inspecció General de Serveis i del sistema d'alertes per a la prevenció de males pràctiques en l'Administració de la Generalitat i el seu sector públic instrumental, regula el sistema d'alerta —conegut com *SALER*, de «Sistema de Alertas Tempranas»— al Cap. I del seu Títol II. Tractarem en detall el sistema SALER en l'apartat 3.2 d'aquest estudi.

En tots aquests casos és procedent parlar d'alertes: els indicadors de risc faciliten informació, tant a escala macroscòpica com microscòpia, indicativa del nivell de riscos potencials i per tant, quan indiquen un risc elevat, indiquen una alta probabilitat que es produeixi algun tipus d'irregularitat; els sistemes en temps real alerten, en alguns casos, d'irregularitats efectives o, en d'altres, d'un alt nivell de risc en procediments concrets; i, com el seu propi nom indica, els alertadors posen en coneixement de les autoritats de control, internes o externes, de situacions irregulars o fins i tot de frau o corrupció de les que puguin tenir coneixement.

Tots són, literalment parlant, sistemes d'alerta; i tots són igualment necessaris: són les diverses peces que, juntament amb d'altres, integren un sistema d'integritat [6].

En aquest document, però, ens centrarem en **sistemes d'alerta basats en dades i processos de tractament automatitzat de les mateixes**.

Els sistemes d'alerta que aquí considerem es podrien definir doncs com a sistemes tecnològics que, mitjançant els corresponents algoritmes processen dades de diverses fonts, tant intrínseques als procediments de contractació com extrínseques als mateixos, detecten i posen automatitzadament en coneixement de les instàncies de control, internes i/o externes, l'existència o la possibilitat —i, eventualment, en aquets casos, la probabilitat— d'irregularitats i, en el seu cas, n'impedeixen l'efectiva materialització.

[6] Des d'aquesta perspectiva àmplia, l'article monogràfic *La función de los sistemas de alerta en la gestión de riesgos para la integridad: ¿prevención o contingencia?* de Roger FOLGUERA FONDEVILLA i per Lara BAENA GARCÍA, cap de l'Àrea de Generalitat i Parlament de la Direcció d'Investigacions i consultora de la Direcció de Prevenció de l'Oficina Antifrau, respectivament, publicat al núm. 9, de gener-abril de 2019, de la *Revista Internacional de Transparencia e Integridad* i accessible a: http://www.encuentros-multidisciplinares.org/revista-65/roger-folguera_y_lara-baena.pdf, on s'analitzen acuradament els 4 dels sistemes d'alerta als quals s'ha fet referència —sistema SALER de la Comunitat Valenciana, eina Arachne de la Comissió Europea, el sistema MET (*Monitoring European Tender*), derivat del projecte DIGIWHIST, i projecte hongarès Red Flags—, incideix en les seves conclusions en la necessitat de complementar els *sistemes d'alerta* existents amb «les informacions provinents d'alertadors o *whistleblowers*».

2 Diagnosi

2.1 Context general

L'esmentat concepte de sistemes automatitzats d'alerta en l'àmbit de la contractació pública, entès i definit en els termes que acabem de veure i que aquí considerem, s'ha de situar en un context més ampli, que no és un altre que el de la **digitalització de l'activitat** general **del sector públic** i, específicament, de l'activitat de contractació pública.

En els següents apartats, repassarem breument el marc normatiu en el qual es fonamenta aquest element contextual, els paradigmes que n'han impulsat el desenvolupament, i la conseqüència fenomenològica que ha generat.

2.1.1 Marc normatiu: procediment electrònic i contractació electrònica

Tot i que ja existien diversos antecedents normatius —que presentaven, però, un cert grau de dispersió i, per tant, plantejaven problemes de coherència entre els diversos règims superposats—, és la Llei 39/2015, de l'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques (LPAC) la que estableix els fonaments i els **elements essencial que possibiliten la tramitació electrònica dels procediments administratius**: signatura electrònica, registre electrònic d'apoderaments, registre electrònic i notificacions electròniques a través del punt d'accés general electrònic de l'administració que opera com a portal d'entrada, seu electrònica, arxiu electrònic únic d'expedients de procediments finalitzats; registre d'empleats públics habilitats, etc.

De fet, la LPAC no es limita a regular aquests elements que possibiliten la tramitació electrònica dels procediments; tal i com afirma a l'apartat III de la seva exposició de motius:

> *«... en l'entorn actual, **la tramitació electrònica** no pot ser ja una forma especial de gestió dels procediments, sinó que **ha de constituir l'actuació habitual de les Administracions**.»*

Més concretament, l'exposició de motius de la LPAC, en referir-se al títol IV de la llei, sobre el procediment administratiu comú, destaca com la regulació «incorpora a les fases d'iniciació, ordenació, instrucció i finalització del procediment l'ús generalitzat i obligatori de mitjans electrònics», i preveu igualment «la regulació de l'expedient administratiu establint el seu format electrònic i els documents que l'han d'integrar».

La LPAC preveia que els referits elements estructurals fonamentals que havien de permetre l'existència i la tramitació, real i efectiva, de procediments electrònics, estiguessin operatius a finals de 2018. Així, la disp. final 7a de la LPAC, en la redacció originària, preveia l'entrada en vigor de «les previsions relatives al registre electrònic d'apoderaments, registre electrònic, registre d'empleats públics habilitats, punt d'accés general electrònic de l'Administració

i arxiu únic electrònic [...] als dos anys de l'entrada en vigor de la Llei», és a dir, el 02/10/2018[7].

La constatació, per part del legislador, de la impossibilitat de complir aquest termini per part de moltes administracions públiques —especialment per les administracions locals—, va determinar que la disp. final 7a de la LPAC fos modificada, en un primer moment, pel RD-L 11/2018, de 31 d'agost, de modificació, entre d'altres, de la LPAC. La nova data d'entrada en vigor de les previsions de la LPAC relatives al procediment electrònic passava a ser el 02/10/2020.

I finalment, una nova modificació de la disp. final 7a LPAC, primer pel RD-L 27/2020, de 4 d'agost, de mesures financeres, de caràcter extraordinari i urgent, aplicables als ens locals, i, en ser revocada aquella disposició per manca de convalidació del Congrés dels Diputats[8], pel RD-L 28/2020, de 22 de setembre, de treball a distància, que finalment esdevindria la Llei 10/2021, de 9 de juliol, va fixar la data d'entrada en vigor el 02/04/2021.

Les previsions normatives no fan aparèixer per si soles els mitjans per complir-les —especialment quan aquests mitjans són tecnològics i la seva implantació i posada en funcionament, amb els grans canvis organitzatius i operatius que això comporta, és particularment complexa—. I, com veurem més endavant, no es pot afirmar que totes les administracions facin un «ús generalitzat i obligatori de mitjans electrònics», com pretenia la LCAP.

No obstant, davant la imminència de l'esmentada entrada en vigor de les referides previsions de la LCAP, es va publicar al BOE de 31/03/2021, el RD 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics (RAFME), que desenvolupa les disposicions de la LCAP. L'exposició de motius del RAFME incideix en la necessitat de «comptar amb un marc regulatori adequat, [...], que tot garantint la seguretat jurídica per a tots els intervinents serveixi els objectius de millorar l'eficiència administrativa per tal de fer efectiva una Administració totalment electrònica i interconnectada, incrementar la transparència de l'actuació administrativa i la participació de les persones en l'Administració Electrònica i garantir serveis digitals fàcilment utilitzables». I així, al servei d'aquests quatre grans objectius —«millorar l'eficiència administrativa, incrementar la transparència i la participació, garantir serveis digitals fàcilment utilitzables i millorar la seguretat jurídica»—, i sota els principis generals de neutralitat i adaptabilitat als progressos tecnològics, d'accessibilitat, de facilitat d'ús, d'interoperabilitat, de proporcionalitat i de personalització i proactivitat, proclamats al seu art. 2, el RAFME regula detalladament:

a. al seu títol I, els **portals d'Internet**, els **punts d'accés general electrònics** i les **seus electròniques** de les diverses administracions públiques, així com

[7] La LPAC va ser publicada al BOE de 02/10/2015, i la seva disp. final 7a en preveia l'entrada en vigor, amb caràcter general, a l'any de la seva publicació: el 02/10/2016.

[8] Resolució de 10/09/2020, que publica l'acord del Congrés dels Diputats pel qual es deroga el RD-L 27/2020, de 4 d'agost.

l'**àrea personalitzada** per a cada interessat, coneguda com a ***carpeta ciutadana***;

b. al títol II, el **procediment administratiu electrònic** i els seus elements principals: identificació i autenticació, registres electrònics i notificacions i comunicacions electròniques;

c. al títol III, l'**expedient electrònic**, incidint en els documents administratius electrònics i la seva conservació, i en el concepte d'arxiu electrònic únic; i

d. finalment, al títol IV, la **col·laboració** i les **relacions entre administracions públiques**, la interconnexió de registres —que pressuposa la seva interoperabilitat—, la remissió electrònica d'expedients i l'intercanvi i transmissió de dades.

A Catalunya, el Decret 76/2021, de 4 d'agost, d'Administració digital (DAD) ha reprès i adaptat a les singularitats i especificitats del marc normatiu català moltes de les disposicions del RAFME de desenvolupament normatiu de la LCAP en l'àmbit que ens ocupa —cal tenir present que el RAFME té, majoritàriament, caràcter bàsic, com precisa la seva disp. final 1a—. El DAD, però, va més enllà i, des d'una perspectiva més àmplia i ambiciosa, incideix en el concepte de **governança de les dades**. A aquest respecte, a la seva exposició de motius destaca el següent:

> *«... el règim jurídic relatiu als mitjans electrònics en l'àmbit de l'Administració de la Generalitat i del seu sector públic requereix una adaptació a la nova situació legal i fàctica. Aquesta adaptació reclama una nova norma que incorpori **no només les determinacions necessàries per fer efectiu el funcionament electrònic ordinari**, sinó **també el model de relació i utilització de les noves tecnologies** més adient, eficaç, eficient, transparent i obert que sigui possible, en atenció al marc social i econòmic sobre el qual s'ha de projectar.*
>
> *Partint d'aquesta necessitat d'actualització normativa, la previsió d'**un govern de les dades** adient ha de constituir un dels pilars fonamentals d'allò que ha de ser l'Administració digital de la Generalitat. En aquest sentit, [...], és determinant establir **un model de dades propi**, en la mesura que la gestió documental i arxivística de la informació digital s'estructura sobre les dades, per tal d'estructurar la documentació administrativa digital de la manera més adequada.*
>
> ***El govern de les dades**, més enllà de l'ús de les dades en el marc de la gestió dels actius digitals, **permet crear nous serveis digitals analítics i predictius** utilitzant les tecnologies més avançades, que són determinants per a la millora contínua de la prestació dels serveis públics.»*

Conseqüentment, després d'establir al seu títol I l'objecte, l'àmbit d'aplicació, les finalitats i els principis generals informadors d'aquesta norma, així com les estructures organitzatives de governança de l'Administració digital, el cap. I del títol II del DAD regula el **model de govern de dades**, definit a l'art. 10.1 com «l'instrument organitzatiu que determina els criteris i elements que defineixen el govern de les dades a l'Administració de la Generalitat», el desplegament del

qual «es realitza mitjançant **un protocol**[9], que és el document que recull els aspectes tècnics i organitzatius necessaris per implantar-lo». Aquest model de govern de dades pressuposa i es fonamenta en una sèrie de premisses:

a. en primer lloc, que «**Les dades són un *actiu digital* compartit** per tots els subjectes [als quals és d'aplicació el DAD] [...], per la qual cosa **se n'ha de maximitzar la reutilització**» —art. 10.2 a) del DAD—;

b. que el model de govern de dades ha de ser **comú** tot i **adaptar-se a les necessitats específiques** de cada ens o unitat orgànica —art. 10.2 b)—, incloure «totes les dades fonamentals i totes les dades de les àrees de gestió sectorials» i ajustar-se «a la complexitat de les activitats de l'àrea i les necessitats de les persones, segons el principi de proporcionalitat» —art. 10.2 c)—;

c. que «La gestió basada en dades es fonamenta en e**stàndards que garanteixen l'homogeneïtat semàntica i sintàctica de les dades**»[10] —art. 10.2 d)— i que «Les dades comuniquen la informació de manera clara i concisa, proporcionant informació significativa per facilitar una presa de decisions» —art. 10.2 e)—;

d. que el model de govern de dades ha de garantir:

   i. «el criteri de **dada única** a través de la col·laboració entre els òrgans i sistemes custodis d'una mateixa dada i la identificació unívoca de la font més fiable, si s'escau, en origen» —art. 10.2 f)—, i

   ii. «la **seguretat** de les dades, gestionant-ne l'alta, modificació, consulta i supressió de manera segura i amb traçabilitat, així com l'**autenticitat, integritat, confidencialitat, privacitat i disponibilitat**» —art. 10.2 g)—;

e. finalment, que el model de govern de dades ha de respectar «els principis i requeriments previstos en el marc de la normativa vigent de **protecció de dades, transparència i accés a la informació, i estadística**», i garantir-ne «la interoperabilitat i la reutilització» —art. 10.4 del DAD—.

En definitiva, aquesta normativa catalana no només ha desenvolupat les previsions generals de la LCAP a nivell operatiu i procedimental sinó que ha definit i establert un marc conceptual i normatiu que estableix les bases d'una

[9] L'art. 11 del DAD regula el contingut mínim del protocol de govern de les dades que ha d'incloure els elements següents: «a) Rols i responsabilitats de les persones i organismes que intervenen en el model de gestió de les dades. b) Qualitat de les dades. c) Cicle de vida de les dades. d) Modelització i arquitectura de les dades. e) Seguretat. f) Metadades. g) Catàleg de dades. h) Analítica de dades. i) Sistemes d'avaluació i seguiment del model de govern de les dades», conceptes, tots ells, definits al glossari de l'annex 2 del DAD.

[10] Aquest concepte d'*homogeneïtat semàntica i sintàctica de les dades* ve igualment definit al glossari de l'annex 2 del DAD en els termes següents: «condició per la qual **les dades tenen el mateix significat** per a totes les unitats i òrgans de l'Administració **i s'ordenen i es relacionen entre si de la mateixa manera**». Es tracta, en definitiva, d'assegurar que les dades obtingudes i gestionades per una unitat orgànica integrant del model puguin ser utilitzades amb la màxima facilitat, eficàcia i eficiència per qualsevol altra unitat.

veritable política de gestió i governança de les dades, alineant-se amb les millors pràctiques internacionalment reconegudes [11].

Aquests són els principals elements que integren el marc jurídic general regulador del procediment electrònic.

Si considerem ara, específicament, l'àmbit de la **contractació pública**, podem afirmar que és probablement **un dels àmbits d'activitat del sector públic on la digitalització s'ha desenvolupat més intensament**. En això ha estat determinant un doble imperatiu normatiu coincident:

a. de la normativa europea: Directiva 2014/24/UE del Parlament Europeu i del Consell, de 26 de febrer de 2014, sobre contractació pública i per la qual es deroga la Directiva 2004/18/CE, i

b. de la normativa estatal de transposició de l'anterior: la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic (LCSP).

Cal remarcar, però, que la digitalització de l'activitat de contractació pública ja havia començat molt abans.

La Generalitat de Catalunya va ser pionera en aquest àmbit: abans, fins i tot, de la promulgació de la directiva de 2004, va regular, mitjançant el Decret 96/2004, de 20 de gener, la utilització dels mitjans electrònics, informàtics i telemàtics en la contractació. Aquest decret va constituir el marc normatiu sota el qual es va començar a construir el Sistema corporatiu de contractació pública electrònica de Catalunya [12], que ha anat integrant els diversos elements que possibilitaven, de forma gradualment més i més intensa, la digitalització de l'activitat contractual de la Generalitat: registre de licitadors, gestor electrònic de contractació, plataforma de contractació, registre públic de contractes, etc.

D'altra banda, va constituir una fita molt rellevant, al seu moment, la creació, per l'art. 42 de la Llei 30/2007, de 30 d'octubre, de contractes del Sector Públic, del **perfil de contractant** com a eina de difusió i publicitat a Internet d'anuncis, informació i dades de contractació pública de les entitats del sector públic.

Però si l'anterior Directiva 2004/18/CE —coneguda com a directiva clàssica de contractació pública, la transposició de la qual al nostre ordenament va ser precisament l'esmentada Llei 30/2007— apostava decididament per l'ús intensiu dels mitjans electrònics en els procediments de contractació, la regulació establerta en la nova directiva clàssica 2014/24/UE representà un

[11] El document de la OCDE *Analytics for Integrity. Data-driven approaches for enhancing corruption and fraud risk assessments* (OECD, 2019) —accessible a: https://www.oecd.org/gov/ethics/analytics-for-integrity.pdf—, de referència en l'àmbit que ens ocupa, incideix reiteradament en la importància, per a la implementació i desenvolupament de qualsevol estratègia general o projecte concret basat en dades (*data-driven*), de l'existència d'una **cultura i governança de dades** sòlidament implantades i arrelades a nivell institucional: «... l'efectivitat de l'anàlisi de dades en qualsevol context requereix una eficaç governança institucional així com **una bona governança de dades**, dades íntegres i una bona planificació a nivell de projectes».

[12] Una descripció de la configuració actual del Sistema i dels elements que l'integren es pot trobar a: https://contractacio.gencat.cat/ca/contractacio-electronica/.

veritable salt qualitatiu en aquest àmbit, en la mesura que preveia, una vegada transcorregut un període transitori de 30 mesos, **la implantació generalitzada de la licitació íntegrament electrònica dels contractes públics**: l'***e-procurement***, és a dir, l'ús dels mitjans electrònics en totes les fases del procediment de contractació[13] —anuncis de licitació, posada a disposició dels potencials licitadors de tota la documentació corresponent, presentació de les sol·licituds de participació i de les ofertes, resolució...—. Tal i com indiquen els apartats (52) i (80) del preàmbul de la Directiva 2014/24/UE, els objectius són simplificar la publicitat de les licitacions i fer els procediments de contractació més eficaços i transparents, facilitant l'accés dels diversos operadors econòmics i, especialment, de les pimes.

L'evolució en aquest àmbit de la directiva clàssica de 2004 a la vigent de 2014 és molt significativa. Si un dels objectius explícits de la primera era situar en condicions d'igualtat els mitjans electrònics i els mitjans clàssics de comunicació —paràgraf (35) del preàmbul—, el que pressuposava que aquests últims eren els mitjans usuals de comunicació entre operadors econòmics i poders adjudicadors, en la Directiva 2014/24/UE **l'ús de mitjans electrònics** —definits al seu art. 2.1.19— **esdevé la regla general** —art. 22—.

I tal i com ho anuncia el paràgraf (52) del preàmbul, l'art. 90 de la directiva que regula la seva transposició estableix l'obligació per a tots els Estats membres d'implantar l'*e-procurement* previst a l'art. 22 al més tard el 18/10/2018 —30 mesos després de la finalització del termini de transposició de la directiva, el 18/04/2016—.

En aquest sentit, cal destacar especialment les disposicions de la directiva següents:

a. les previsions relatives a la interoperabilitat —paràgrafs (55) i (56) del preàmbul—, i a la seguretat —paràgraf (57) del preàmbul— dels mitjans electrònics, així com a la preservació de la integritat i la confidencialitat de les dades, establertes a l'art. 22 de la Directiva 2014/24/UE;

b. l'obligació per a tots els poders adjudicadors de posar a disposició dels operadors econòmics els documents de licitació —plecs de clàusules i demés documentació— per mitjans electrònics, en els termes establerts a l'art. 53 de la directiva, obligació no sotmesa al període transitori de 30 mesos abans esmentat i, per tant, en vigor des de la finalització del termini de transposició de la directiva, el 18/04/2016, *ex* art. 90.2 *in fine*;

c. la possibilitat, durant el període transitori —i, per tant, abans de la generalització de l'*e-procurement*—, per aquells poders adjudicadors que admetin la licitació electrònica, de reduir els terminis mínims de presentació d'ofertes —arts. 27.4 i 28.5—; i

[13] En paraules de la presentació de la política d'*e-procurement* al web oficial de la Comissió Europea —accessible a: https://ec.europa.eu/growth/single-market/public-procurement/digital-procurementes—: «La contractació pública està experimentant una transformació digital. La UE dona suport al procés de **repensar el procediment de contractació pública tenint present les tecnologies digitals**. Això va més enllà de simplement fer ús d'eines electròniques...».

d. la previsió de l'art. 59.2 que preveu que el Document europeu únic de contractació (DEUC) que permet als licitadors acreditar que compleixen els requisits i criteris de selecció qualitativa per poder participar a les licitacions només podrà facilitar-se en format electrònic.

Com hem vist, el termini general de transposició de la directiva clàssica de contractació 2014/24/UE finalitzava el 18/04/2016, amb l'excepció, entre d'altres, de les previsions sobre contractació electrònica de l'art. 22, el termini de transposició de les quals finalitzava el 18/10/2018. Això no obstant, no va ser fins al 09/11/2017 que es va publicar al BOE la vigent LCSP que transposava finalment, ja fora de termini, la directiva. D'acord amb la seva disp. final 16a, la LCSP entrava en vigor als 4 mesos de la seva publicació, és a dir, el 09/03/2018, cosa que l'exposició de motius de la llei qualifica —en un to potser excessivament autocomplaent— de mostra de «la decidida aposta […] [del] nou text legal […] a favor de la contractació electrònica, establint-la com a obligatòria en els termes que s'hi indiquen, des de la seva entrada en vigor, anticipant-se, per tant, als terminis previstos a nivell comunitari».

2.1.2 Nous paradigmes: transparència i dades obertes

El marc normatiu que acabem de descriure a grans trets no ha estat, però, l'únic factor que ha impulsat el desenvolupament de la digitalització de la contractació pública. També hi han contribuït la progressiva implantació, tant a nivell legal com operatiu, de dos grans paradigmes íntimament relacionats: **la transparència i les dades obertes**.

En el pla normatiu, la introducció d'aquests paradigmes en el nostre ordenament jurídic es produeix amb la promulgació de les lleis de transparència: Llei estatal 19/2013, del 9 de desembre, i Llei catalana 19/2014, del 29 de desembre, de transparència, accés a la informació pública i bon govern, que imposen a totes les administracions públiques obligacions de publicitat activa en matèria d'organització i estructura administrativa, dades econòmiques, pressupostàries i de patrimoni, decisions i actes rellevants, plantilla i llocs de treball, procediments administratius, contractes i convenis, subvencions, informes, plans i programes, i dades estadístiques i geogràfiques (art. 8 de la Llei 19/2014), preveient explícitament que les dades siguin publicades en el corresponent Portal de transparència (art. 5.4 de la Llei 19/2014) en formats explotables i reutilitzables (art. 16 de la Llei 19/2014).

La introducció al nostre ordenament d'aquest règim de transparència té una importància cabdal i comporta una veritable revolució, d'abast autènticament global.

Així, a la seva obra *Hacia el Derecho Administrativo Global: fundamentos, principios y ámbito de aplicación*[14], els autors, Richard B. STEWART i Benedict KINGSBURY, professors de la Universitat de Nova York, identifiquen els principis següents, vertebradors d'un nou i emergent Dret públic global: el retiment de comptes, la participació, la transparència, la motivació i el control.

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

Tres d'ells —tots tres, de fet, profundament vinculats a la missió de l'Oficina Antifrau—, el retiment de comptes, la transparència i el control es projecten sobre i es concreten en el que es coneix com a governança basada en **dades obertes**. Els imperatius derivats de les lleis de transparència obliguen al sector públic a fer públiques dades sobre la seva estructura, el seu funcionament i la seva activitat; aquestes dades, que són una forma de retiment de comptes, poden ser utilitzades per la ciutadania en el marc dels processos de participació millorant i enriquint els processos de decisió pública i, més generalment, són considerades un actiu intangible d'alt valor estratègic —ja hem vist que així ho explicita l'art. 10.2 a) del DAD: cfr. apartat 2.1.1 anterior—.

El caràcter i l'abast global d'aquest moviment és palès si considerem els diversos documents internacionals que li donen suport.

Així, precisament l'any 2014 el Consell de l'OCDE va aprovar la *Recomanació sobre estratègies de govern digital*[15] que constitueix el primer instrument legal internacional sobre el govern digital. En la presentació d'aquest document s'apunta que «el repte no és la introducció de les tecnologies digitals en les administracions públiques; és integrar el seu ús en els esforços de modernització del sector públic», i que del que es tracta és d'evolucionar cap a l'«ús de la tecnologia per modelar els resultats de la governança pública, i no simplement per donar suport als processos administratius de govern». I coherentment, l'apartat II.3 de la recomanació incideix en la necessitat de **«crear una cultura basada en dades en el sector públic»**.

Igualment, el G20, a la seva 10a cimera, celebrada a Antalaya (Turquia) al novembre de 2015, va aprovar el document *Principis de dades obertes anticorrupció*[16], a la nota introductòria del qual s'indica el següent:

> *«Aquests Principis han estat desenvolupats tenint en compte estàndards internacionals, bones pràctiques i es fonamenten en tres idees bàsiques:*
>
> *1. El progrés exponencial de les tecnologies digitals i l'increment sense precedents de la quantitat, les fonts i la qualitat de les dades disponibles i dels estàndards comuns de dades ofereixen l'entorn adequat i les eines necessàries per promoure la disponibilitat i l'**ús de les dades obertes en la lluita contra la corrupció**.*
>
> *2. La transparència és primordial en la lluita contra la corrupció i ambdues es poden reforçar mútuament a través d'una col·laboració activa basada en la disponibilitat i l'ús de les dades obertes; i*
>
> *3. Com a tal, **les dades obertes contribueixen a la prevenció, la detecció, la investigació i la reducció de la corrupció**.»*

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

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

Partint d'aquestes premisses, el G20 va assumir el conjunt de principis en els quals es basa la *Carta internacional de Dades Obertes*[17], que estableixen que les dades han de ser: obertes per defecte; actualitzades i exhaustives; accessibles i utilitzables; comparables i interoperables; per millorar la governança i la participació ciutadana; i per al desenvolupament inclusiu i la innovació.

El paradigma de la governança basada en dades obertes es troba hores d'ara positivitzat en el nostre ordenament jurídic tant a nivell europeu com a nivell nacional.

A nivell europeu, la Directiva (UE) 2019/1024 del Parlament Europeu i del Consell del 20 de juny de 2019, relativa a les dades obertes i la reutilització d'informació del sector públic, el termini de transposició de la qual finalitzava el 17/07/2021, estableix un marc normatiu mínim general i formula en el seu preàmbul (apartats 8è, 13è, 14è i 16è) les declaracions següents:

> *«El sector públic dels estats membres recopila, produeix, reprodueix i difon un ampli ventall d'informacions en un gran nombre d'àmbits d'activitat, [...]. Els documents produïts pels organismes del sector públic que integren el poder executiu, legislatiu o judicial constitueixen una reserva de recursos àmplia, diversificada i molt valuosa, de la qual la societat es pot beneficiar. El fet de posar a disposició aquestes informacions, que inclouen dades dinàmiques, en un format digital d'ús corrent permet a la ciutadania i a les persones jurídiques trobar-los els nous usos i crear nous productes i serveis innovadors. [...]*
>
> *Les informacions del sector públic o aquelles recopilades, produïdes, reproduïdes i difoses en l'exercici d'una missió de servei públic o d'un servei d'interès general constitueixen una matèria prima important per als productes i els serveis de naturalesa digital i esdevindran un recurs més i més important en quan el seu contingut a mesura que les tecnologies digital de punta, com la intel·ligència artificial, els registres distribuïts o l'internet dels objectes es vagin desenvolupant. [...]*
>
> *Autoritzar la reutilització de documents detentats per un organisme del sector públic genera valor afegit en benefici dels reutilitzadors, dels usuaris finals, de la societat, en el seu conjunt i, en molts casos, en benefici de l'organisme del sector públic mateix, en afavorir la transferència i la responsabilitat i en permetre el retorn d'informacions dels reutilitzadors i dels usuaris finals, el que permet a l'organisme del sector públic concernit millorar la qualitat de les informacions recopilades en l'exercici de les seves missions. [...]*
>
> *El concepte de **dades obertes** s'entén generalment com designant dades presentades en un format obert que poden ser lliurement utilitzades, reutilitzades i compartides per tots qualsevol que en sigui la finalitat. Les polítiques en matèria de dades obertes [...], poden jugar un rol important per promoure el compromís social, i promoure i recolzar el*

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

desenvolupament de nous serveis basats en formes innovadores de combinar i utilitzar aquestes informacions.»

I a nivell català, el govern de la Generalitat va aprovar l'acord GOV/154/2018, de 20 de desembre [18], pel qual s'aprova l'estratègia de dades obertes de la Generalitat de Catalunya i l'adhesió a la Carta Internacional de Dades Obertes.

2.1.3 Marc conceptual: la datificació al servei de la integritat

En aquest marc legal i sota aquests paradigmes, s'ha estès al sector públic el fenomen conegut com a **datificació** [19] de l'activitat pública, que podríem definir com «el procés de captar tots els aspectes de la vida i transformar-los en dades» [20].

És notori que el fenomen de la datificació s'ha produït i estès en molts àmbits de la vida individual i col·lectiva —social, econòmica i política— en la nostra societat. Però es produeix igualment —i això és el que aquí ens ocupa— en l'àmbit de l'activitat del sector públic.

En la vida privada la datificació és una conseqüència directa de l'ús cada vegada més intensiu de mitjans electrònics de comunicació —paradigmàticament els telèfons intel·ligents que, més enllà de permetre comunicar-nos, són un dels principals canals d'accés a les xarxes socials i a Internet, i ens permeten dur a terme tota classe des gestions particulars, econòmiques, administratives, financeres o de qualsevol altra naturalesa—; aquest ús genera dades que són massivament recopilades i explotades pels operadors i intermediaris amb què interaccionem [21].

En el sector públic, retrobem aquest mateix fenomen, que s'estén cada vegada més ràpidament i intensa, impulsat per les dues forces que hem esmentat fins aquí:

---

[18] Publicat al DOGC de 27/12/2018.

[19] Es sol considerar introductors del neologisme *datificació* a Kenneth CUKIER i Viktor MAYER-SCHOENBERGER en el seu article publicat al núm. de maig-juny de 2013 de la revista *Foreign Affairs* titulat *The Rise of Big Data* (*L'emergència del* Big Data).

[20] Citem aquí l'obra introductòria a la ciència de dades *Doing Data Science*, de Rachel SCHUTT i Cathy O'NEIL (ed. O'Reilly, 1a ed., octubre 2013; pàg. 5 i 6), que recullen la definició del concepte de CUKIER i MAYER-SCHOENBERGER i n'analitzen críticament les implicacions.

[21] En la seva obra esmentada —cfr. nota anterior—, SCHUTT i O'NEIL analitzen les implicacions de la datificació en l'àmbit privat, remarcant al respecte:

a. per una banda, que «la datificació és un concepte interessant que ens porta a considerar-ne la importància en relació amb la intencionalitat de la gent a l'hora de compartir les seves pròpies dades», destacant que no sempre assumim conscientment i voluntària que moltes de les nostres accions en contextos i a través de mitjans electrònics siguin datificades;

b. i, conseqüentment, qüestionant les conseqüències i corol·laris que CUKIER i MAYER-SCHOENBERGER extreuen de la definició de datificació —«Una vegada que hem datificat les coses, podem transformar la seva utilitat convertint la informació en noves formes de valor»—, que cal interrogar-se sobre qui du a terme aquesta transformació, quines són aquestes noves formes de valor, i, òbviament, qui se'n beneficia.

a. d'una banda, directament, la tramitació electrònica dels procediments administratius comporta la generació directa de dades emmagatzemades —de forma més o menys automatitzada i més o menys fàcilment recuperables i, per tant, explotables— en el propi expedient electrònic i els documents electrònics que l'integren, així com, eventualment, a les aplicacions de gestió que suporten i faciliten la tramitació;

b. d'altra banda, indirectament, els imperatius derivats tant de la transparència com de la progressiva implantació i desenvolupament del paradigma de les dades obertes obliguen els organismes i entitats del sector públic a recopilar *en suports electrònics* determinades dades —les que han de ser objecte de publicitat activa, com a mínim—, fins i tot si aquestes dades no es troben en un expedient o document electrònic.

Tant en un cas com a l'altre, el resultat final és que cada vegada l'activitat del sector públic genera més dades en suports electrònics i, per tant, fàcilment recopilables, emmagatzemables, tractables i explotables per a molt diverses finalitats. Paral·lelament, l'última dècada ha vist incrementar-se exponencialment les capacitats tècniques d'emmagatzematge i d'explotació d'aquesta ingent quantitat de dades, amb un cost cada vegada més reduït.

Les finalitats al servei de les quals es pot posar aquesta capacitat exponencialment creixent de recopilació, emmagatzematge i anàlisi de les dades generades pel sector públic són múltiples:

a. tradicionalment —al sector privat molt abans que al públic—, l'anàlisi de dades ha servit en primer lloc com a eina al servei de la **presa de decisions** de gestió operativa o estratègica;

b. estretament vinculada a l'anterior —de fet, n'és una concreció—, una altra finalitat és l'**optimització de l'ús de recursos limitats**: el coneixement i l'eventual previsió, sobre una base empírica i quantitativa, dels efectes i de l'impacte de les decisions d'assignació dels recursos disponibles permet avaluar-les i, en una dinàmica cíclica —per exemple la dels processos anuals d'elaboració pressupostària—, optimitzar-les;

c. més recentment, l'ús d'eines d'anàlisi massiu de dades i d'aprenentatge automàtic s'està fent servir per **personalitzar proactivament els serveis públics electrònics** oferts a la ciutadania [22];

d. i, evidentment, la datificació del sector públic ha de posar-se, inexcusablement, **al servei de la integritat**, permetent i facilitant la prevenció, detecció, correcció i persecució d'irregularitats i, en el seu cas, de supòsits de frau i/o de corrupció.

[22] La *Recomanació sobre estratègies de govern digital* de l'OCDE de 2014, ja citada —cfr. nota 15 anterior—, destaca en la seva introducció precisament la conveniència pels poders públics de «reorganitzar-se al voltant de les expectatives, necessitats i requisits associats dels usuaris [dels serveis públics], més que centrant-se en les seves pròpies lògiques i necessitats».

I de fet l'art. 4 c) del DAD enumera entre els principis generals de l'administració digital precisament el de «Proactivitat i personalització en la prestació de serveis públics digitals amb l'objectiu de situar l'experiència de les persones en el centre del disseny de serveis».

Aquesta idea de posar la datificació del sector públic al servei de la integritat constitueix el nucli d'un document que podem considerar una referència essencial en aquest àmbit: el document de la OCDE *Analytics for Integrity. Data-driven approaches for enhancing corruption and fraud risk assessments (Eines analítiques per a la Integritat. Aproximacions basades en dades per una millor avaluació del risc de frau i corrupció)*[23].

El document parteix dels principis, bones pràctiques i metodologies clàssiques d'avaluació de riscos i constata que l'«adveniment de l'edat digital en el govern ha generat noves oportunitats per a l'avaluació dels riscos de frau i corrupció», contraposant les **tècniques o aproximacions qualitatives** d'avaluació de riscos de frau i corrupció, basades en percepcions humanes dels subjectes implicats —i, correlativament, en llur sensibilització i formació—, amb les **aproximacions quantitatives**, basades en les dades i en la utilització d'eines analítiques[24], i destaca reiteradament que **les aproximacions qualitatives i quantitatives són recíprocament complementàries**[25].

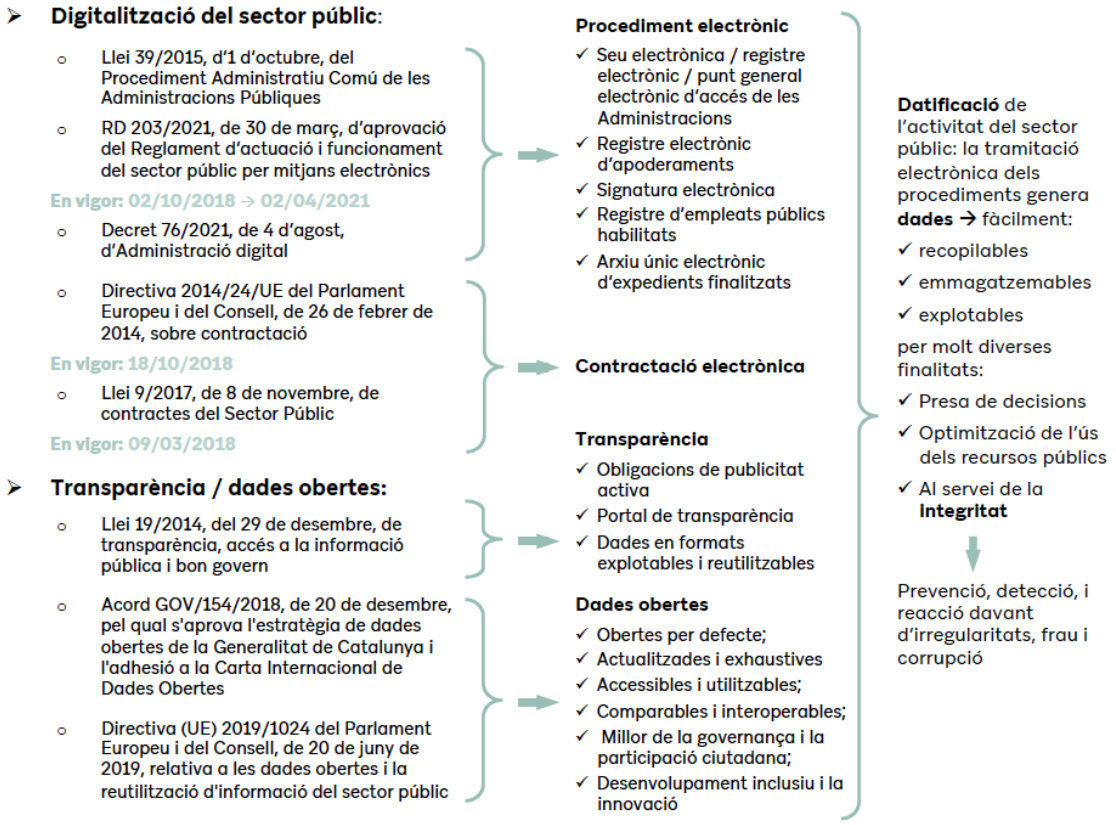
Partint d'aquesta premissa, s'exposen i analitzen els passos a seguir per a la «creació d'un pla d'anàlisi de dades amb objectius específics d'integritat i la selecció de les tècniques més adients d'acord amb aquests objectius i els recursos disponibles». A partir de l'experiència concreta del desenvolupament d'un projecte basat en dades d'avaluació i gestió de riscos en grans projectes d'infraestructures al Grupo Aeroportuario de la Ciudad de México, en el qual va col·laborar l'OCDE, es destaquen la metodologia a seguir, els elements claus, les millors pràctiques i els resultats obtinguts.

Sintetitzant totes aquestes idees en un esquema, tindríem el següent:

[23] Cfr. nota 11 anterior.

[24] *Op. cit.* pàg. 7: «... els gestors de projectes, els gestors de riscos, els responsables de contractació i els òrgans de control, entre d'altres, es basen sovint en **metodologies qualitatives** d'avaluació de riscos [de frau i corrupció] (p. ex. enquestes i entrevistes per a la identificació i ponderació dels riscos). El resultat paradigmàtic d'aquestes aproximacions basades en percepcions són els inventaris i mapes de riscos que mostren la magnitud i la probabilitat dels riscos percebuts. Aquestes aproximacions poden facilitar una comprensió dels riscos més crítics i constitueixen un mitjà efectiu per implicar les persones d'una organització en la gestió de riscos. [...] l'**anàlisi de dades** pot complementar les metodologies qualitatives, i incrementar la comprensió dels riscos existents per part dels gestors i permetre la presa de decisions basades en dades objectives per a la mitigació dels riscos.»; i pàg. 17: «No existeix una metodologia uniforme d'avaluació de riscos, però les aproximacions poden ser, en general **qualitatives, quantitatives o mixtes**. [...] els **mètodes quantitatius** que utilitzen l'anàlisi de dades per avaluar els riscos depenen de la disponibilitat i la qualitat de dades i requereixen sòlides tècniques d'anàlisi.».

[25] *Op. cit.* pàg. 18: «Quan les dades estan disponibles, són fiables i vàlides, els mètodes quantitatius d'avaluació de riscos i l'aplicació de tècniques analítiques poden contribuir a complementar l'avaluació qualitativa implantada en una organització».



2.2 El cigne negre: fons NextGenerationEU

Se sol designar com a cigne negre un esdeveniment que reuneix tres característiques: és totalment imprevist i atípic, fora de l'àmbit de les expectatives raonables; és disruptiu en tant que té un impacte socioeconòmic extrem; i, malgrat la seva raresa, és retrospectivament explicable i racionalitzable [26].

Aquest concepte escau bastant bé per descriure la decisió de les institucions de la UE de crear, a finals de 2020 i principis de 2021, l'instrument temporal de recuperació NextGenerationEU, dotat amb 806.900 milions d'euros, destinat, juntament amb el pressupost a llarg termini de la UE 2021-2027, a fer front a la crisi generada per la COVID-19 i a fomentar la transició cap a una Europa més moderna, sostenible i resilient [27].

No és aquest el lloc d'estudiar en profunditat aquest instrument, però sí que considerarem breument dos aspectes del mateix: els recursos destinats al nostre país a aprofundir i desenvolupar la digitalització de les administracions públiques, per una banda, i, per l'altra, les exigències en matèria d'integritat que han de complir tots els beneficiaris d'aquells fons.

[26] Aquest concepte de *cigne negre* es sol atribuir al filòsof i investigador Nassim Nicholas Taleb, descrit i desenvolupat al seu llibre *The Black Swan. The Impact of Highly Improbable* (*El cigne negre. L'impacte del molt improbable*), Random House, 2a ed. 2010.

[27] Una explicació global i detallada es pot trobar en el document publicat a l'abril de 2021 per la Comissió Europea: *The EU'S 2021-2027 long-term Budget and NextGenerationEU. Facts and Figures*. Accessible a: https://op.europa.eu/es/publication-detail/-/publication/d3e77637-a963-11eb-9585-01aa75ed71a1/language-en.

2.2.1 Recursos

La principal component de l'instrument NextGenerationEU és el Mecanisme de Recuperació i Resiliència (MRR), establert pel Reglament (UE) 2021/241 del Parlament Europeu i del Consell de 12 de febrer de 2021.

En el marc del MRR, el Govern de l'Estat va aprovar el 27/04/2021 el Pla de Recuperació, Transformació i Resiliència (PRTR)[28], que, una vegada tramès a la Comissió Europea, va ser aprovat per aquesta el 16/06/2021.

El PRTR s'estructura al voltant de quatre eixos transversals, un dels quals és el de *Transformació Digital*. Aquests eixos orienten les 10 *polítiques palanca*[29] que articulen les 30 components concretes que integren el Pla. La 4a política palanca, sota el títol *Una Administració per al segle XXI*, inclou una única component, la 11a, denominada: *Modernització de les Administracions Públiques*.

El PRTR preveu una inversió pública de l'ordre de 70.000 milions d'euros el període 2021-2023, estructurada en 20 *programes tractors d'inversió*[30], el tercer dels quals, per ordre de magnitud, és el corresponent a l'esmentada component 11a, de *Modernització de les Administracions públiques*, i té un pressupost total pels exercicis 2021 a 2023 de 4.239 milions d'euros.

En el document complementari de desenvolupament d'aquesta component 11a del PRTR, s'especifiquen els objectius estratègics que inclouen la «digitalització de l'Administració i dels processos», la «modernització de les Administracions públiques, incloent [...], un reforç del marc de contractació pública», i el «reforç de les capacitats administratives». Entre els programes concrets de reformes i d'inversió d'aquesta component, cal destacar els següents:

a. el programa de reforma C11.R4, centrat en la implementació efectiva de l'Estratègia Nacional de Contractació Pública —per cert ja previst i regulat a l'art. 334 de la LCSP— i que incideix, entre d'altres aspectes, en la «transformació digital de la contractació pública», entesa com a «impuls coordinat per a culminar la plena extensió de la utilització de la contractació pública electrònica»;

b. el programa d'inversions C11.I1, de modernització de l'Administració General de l'Estat, que entre d'altres actuacions preveu el desenvolupament d'«eines que permetin digitalitzar el flux de la tramitació dels expedients de contractació, així com eines basades en l'anàlisi de dades i Intel·ligència Artificial que facilitin la gestió dels serveis» mitjançant una iniciativa singular d'*e-procurement*; i

[28] El PRTR, la documentació complementària i de desenvolupament del mateix i la resta de documentació i informació relacionades es poden accedir a: https://planderecuperacion.gob.es/documentos-y-enlaces.

[29] En paraules del PRTR, els 4 eixos transversals —transició ecològica, transformació digital, cohesió territorial i social i igualtat de gènere— «es projecten en 10 polítiques palanca, de gran capacitat arrossegadora de l'activitat i l'ocupació [...], per a impulsar la recuperació econòmica a curt termini i recolzar un procés de transformació que augmenti la productivitat i el creixement potencial de l'economia espanyola en el futur.» (PRTR, versió de 16/06/2021, pàg. 24).

[30] PRTR, versió de 16/06/2021, pàg. 34.

c. el programa d'inversions C11.I3, de transformació digital i modernització de les Administracions autonòmiques i locals; aquest programa preveu uns recursos totals de 578,6 milions d'euros per a les Comunitats Autònomes i de 391,4 milions d'euros per als ens locals, amb els quals es finançaran projectes de modernització alineats amb l'Estratègia Digital 2025[31] i el Pla de Digitalització de l'Administració Pública[32], orientats, entre d'altres, al desenvolupament d'«eines que permetin digitalitzar i homogeneïtzar la tramitació dels expedients i processos de contractació pública per cobrir el procés de contractació de principi a fi, així com ajudar en la presa de decisions mitjançant l'analítica de dades i l'automatització intel·ligent, fomentant l'*e-procurement*».

Destaquem finalment que mitjançant l'Ordre TER/1204/2021, de 3 de novembre, publicada al BOE el 06/11/2021, s'aproven les bases reguladores i es convoquen les subvencions corresponents a aquest últim programa d'inversió. A l'exposició de motius s'indica que dels 391,2 milions d'euros del programa n'estan disponibles 92,77 en el present exercici 2021, amb els quals se subvencionaran projectes de transformació digital i modernització de les administracions de les entitats locals de més de 50.000 habitants o menys que siguin capitals de província —art. 1.1 de l'ordre— fins a l'import màxim assignat a cada entitat a l'annex V de l'ordre —art. 9.3 i .4—.

En l'àmbit català, el Govern de la Generalitat va aprovar el document *Next Generation Catalonia*, que recull els projectes catalans que opten al finançament dels fons NextGenerationEU en el marc del PRTR[33]. El projecte 17è dels 27 inclosos a l'esmentat document s'emmarca en l'eix estratègic E.3, Transformació Digital, i l'àmbit d'actuació A.15, Transformació de les Administracions Públiques, té un pressupost de 210 milions d'euros per al seu primer any d'execució d'un total de 1.120 milions, i preveu com a actors implicats en la seva definició i execució la Generalitat de Catalunya, el Consorci AOC, el Consorci Localret, les Diputacions i universitats catalanes, entre d'altres.

2.2.2 Requisits d'integritat

Es notori que l'execució d'un volum tan important de recursos planteja importants reptes a tots els nivells de les administracions gestores i beneficiàries dels fons NextGenerationEU.

[31] L'agenda España Digital 2025, presentada pel Govern de l'Estat el 23/07/2020, es pot accedir a: https://portal.mineco.gob.es/ca-es/ministerio/estrategias/Pagines/00_Espana_Digital_2025.aspx.

[32] El Pla de Digitalització de les Administracions Públiques 2021-2025, del qual es va informar en el Consell de Ministres el 26/01/2021, es pot accedir a: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Estrategia-TIC/Plan-Digitalizacion-AAPP.html#.Ybsq_y0rz-Y.

[33] El document *Next Generation Catalonia* va ser aprovat pel Govern de la Generalitat el 02/02/2021, juntament amb el DL 5/2021, de 2 de febrer, de mesures per a la implementació i gestió de fons del Mecanisme de Recuperació i Resiliència de la UE.

Es pot accedir a informació sobre l'esmentat document a: https://territori.gencat.cat/ca/detalls/Article/projectes-tes-00001, i al document en sí a: http://economia.gencat.cat/web/.content/20_departament_gabinet_tecnic/arxius/pla-recuperacio-europa/next-generation-catalonia.pdf.

Per establir el marc regulador corresponent, es va publicar al BOE del 30/09/2021 l'Ordre HFP/1030/2021, de 29 de setembre, per la qual es configura el sistema de gestió del PRTR. D'acord amb el seu art. 1.1, aquesta ordre «configura i desenvolupa un Sistema de Gestió orientat a definir, planificar, executar, seguir i controlar els projectes i subprojectes en què es descomponen les mesures (reformes/inversions) previstes als components del Pla de Recuperació, Transformació i Resiliència», i enuncia els principis o criteris de gestió que han d'informar aquest sistema —art. 2.2—, entre els quals cal destacar, als efectes que aquí ens interessen el «reforçament de mecanismes per a la prevenció, detecció i correcció del frau, la corrupció i els conflictes d'interès», principi que es concreta en l'art. 6 que preveu específicament, entre d'altres aspectes:

a. que «tota entitat, decisòria o executora, que participi en l'execució de les mesures del PRTR haurà de disposar d'un "Pla de mesures antifrau" que li permeti garantir i declarar que, en el sèu respectiu àmbit d'actuació, els fons corresponents s'han utilitzat de conformitat amb les normes aplicables, en particular, pel que fa referència a la prevenció, detecció i correcció del frau, la corrupció i els conflictes d'interès» —art. 6.1—;

b. a aquests efectes, l'obligació per a tots els òrgans gestors de dur a terme una avaluació dels riscos de frau —art. 6.4, primer incís—;

c. l'elecció de les mesures de prevenció i detecció adients, a judici de cada òrgan gestor, atenent a les seves característiques específiques —art. 6.4, segon incís—;

d. com a concreció de tot l'anterior, l'aprovació, en un termini inferior a 90 dies des de l'entrada en vigor de l'ordre o des que se'n tingui coneixement de la participació en l'execució del PRTR, d'un Pla de mesures antifrau (PMA) amb el contingut i requeriments mínims establerts a l'apartat 5 de l'art. 6 de l'ordre; i

e. les actuacions a dur a terme en cas que es detecti un possible frau o se'n tingui una sospita raonable —art. 6.6 i .7—.

Cal remarcar que aquestes previsions no fan altra cosa que transcriure en una disposició reglamentària estatal una sèrie de disposicions del Dret europeu que no són gens noves, atès que són aplicables a la gestió dels fons europeus des de fa com a mínim 15 anys [34]. En aquest sentit, no deixa de resultar paradoxal que

[34] Ja al 2006, el Reglament (CE) 1083/2006, del Consell, d'11 de juliol de 2006, que establia les disposicions general comuns als fons europeus (FEDER, Fons Social Europeu, Fons de Cohesió, etc.) imposava als Estats membres, al seu art. 70.1, l'obligació de «prevenir, detectar i corregir les irregularitats i recuperar els imports indegudament satisfets». Per facilitar el compliment d'aquesta obligació, la Comissió Europea va publicar la Nota informativa COCOF/0003/00, sobre indicadors de frau, que formava part de l'Estratègia Conjunta de Prevenció del Frau posada en marxa al 2008.

Posteriorment, l'art. 125.4 c) del Reglament (UE) 1303/2013, del Parlament Europeu i del Consell, de 17 de desembre de 2013, que va derogar i substituir l'anterior, va establir molt més explícitament i clara l'obligació d'«aplicar mesures antifrau eficaces i proporcionades, tenint en compte els riscos detectats» i a aquests efectes la Comissió Europea va publicar la Nota orientativa EGESIF/14/0021/00, de 16/06/2014, sobre avaluació del risc de frau i mesures antifrau efectives i proporcionades.

l'adopció de mesures antifrau sigui —de fet, hagi estat, atès que la normativa europea era de directa aplicació— una **obligació** en la gestió de **recursos públics de la UE** —i, concretament, en la contractació finançada amb fons europeus— però **no ho hagi estat** —i, de fet, segueixi sense ser obligatòria— quan es tracta de la gestió i contractació finançada amb **recursos de la hisenda nacional, autonòmica o locals**.

Per facilitar el compliment d'aquestes disposicions, i «aconseguir una homogeneïtat en el disseny d'aquestes mesures [antifrau] […], i sense perjudici de l'aplicació de mesures addicionals atenent a les característiques i riscos específics de l'entitat de què es tracti» —art. 6.2—, l'ordre facilita, d'una banda, en el seu annex II.B.5 un «Test [de] conflicte d'interès, prevenció del frau i la corrupció» destinat a facilitar l'autoavaluació de riscos i mesures existents per part de les diverses entitats concernides, i, d'altra banda, en el seu annex III.C, una sèrie d'orientacions sobre possibles mesures a adoptar.
Entre les possibles mesures antifrau a les quals fa referència l'ordre, ens interessen especialment les relatives a mecanismes basats en dades:

a. el test d'autoavaluació de riscos i mesures existents conté una única pregunta sobre aquesta qüestió, la 10a: «S'utilitzen eines de prospecció de dades o de puntuació de riscos?», el que indica que, a l'hora d'avaluar els riscos, s'atribueix a aquest aspecte una importància bastant relativa —representa un màxim de 4 punts sobre una puntuació màxima total de 64—;

b. les orientacions de l'annex III.C contenen algunes referències més:

    i. en relació amb la prevenció dels conflictes d'interessos —apartat 1 d) i.C—, es fa referència explícitament a la «comprovació d'informació a través de bases de dades dels registres mercantils, bases de dades d'organismes nacionals i de la UE, expedients dels empleats (tenint en compte les normes de protecció de dades) o a través de la utilització d'eines de prospecció de dades ("*data mining*") o de puntuació de riscos»;

    ii. en relació amb la prevenció i la detecció del frau —apartats 2 b) i.G i 2 b) ii.A—, es fa referència, per a la prevenció, a l'«anàlisi de dades», entesa com «dins dels límits relatius a la protecció de dades, creuament de dades amb d'altres organismes públics o privats del sector que permetin detectar possibles situacions del risc inclús abans de la concessió dels fons»; i per a la detecció, a l'«ús de bases de dades com la Base Nacional de Dades de Subvencions (BNDS), eines de prospecció de dades ("*data mining*") o de puntuació de riscos».

Com es pot veure, les solucions basades en dades i anàlisi de dades tot i ser esmentades com a possible element constituent dels PAM que l'ordre exigeix a tots els òrgans i entitats decisors o executors de mesures o accions del PRTR, no en constitueixen un dels elements centrals, més aviat apareixen amb un cert caràcter residual.

Les previsions de l'Ordre HFP/1030/2021, de 21 de setembre, bàsicament transcriuen part del contingut d'aquella normativa i documentació europea.

Ara bé, el ja esmentat document de l'OCDE *Analytics for Integrity* [35] apunta una idea molt interessant: tractant de determinar la ràtio de beneficis per inversions en sistemes basats en dades i anàlisi de dades, quantificada en termes d'eficàcia en la reducció del frau, fa referència a un estudi dut a terme l'any 2016 per l'Associació d'Examinadors de Frau Certificats (ACFE) que demostra que els sistemes de monitoratge i anàlisi de dades són els que permeten la major reducció de pèrdues per frau respecte d'altres 18 mecanismes de control i detecció —codis de conducta, protecció d'alertadors, auditories externes per sorpresa, estats financers, etc.—. En l'apartat d'aquest estudi dedicat a l'efectivitat dels controls antifrau [36] s'indica que:

> *«... mesurar el valor preventiu dels controls concrets és extremadament difícil, si no impossible. Tot i així, els professionals antifrau sovint han de presentar arguments als gestors per tal d'obtenir recursos addicionals per fer front als riscos de frau. Per ajudar a il·lustrar la rendibilitat dels controls antifrau concrets, hem examinat la mitjana comparada de pèrdues per frau i el temps de detecció de fraus a les organitzacions en funció de cadascun dels 18 controls antifrau existents en el moment en què es va produir el frau.»*

i els quadres comparatius corresponents posen de manifest que **el monitoratge proactiu i l'anàlisi de dades constitueix el mecanisme de control que més redueix les pèrdues per frau** —reducció del 54,0%— dels 18 controls possibles considerats.

Així doncs, i amb base en aquest estudi, l'aposta per mecanismes de prevenció i detecció del frau basats en dades i anàlisi de dades sembla ser de les més interessants, en termes d'eficàcia.

2.3 Situació

Fins aquí hem repassat el que *hauria de ser* —el marc normatiu— i el que *hauria d'arribar a ser* —les perspectives de futur que obren els fons NextGenerationEU—. Però com és la realitat, el que *és*? Quina és la situació real de la digitalització de la contractació pública a Catalunya i dels sistemes automatitzats d'alerta que puguin existir?

2.3.1 Generalitat de Catalunya

La Generalitat de Catalunya disposa des de fa més de 10 anys d'una solució tecnològica per a la tramitació electrònica d'expedients de contractació: el **Gestor electrònic d'expedients de contractació (GEEC)** [37].

[35] Op. cit. pàg. 39. Cfr. notes 11 i 23 anteriors.

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

[37] Es pot accedir a informació sobre el GEEC, a la seva normativa reguladora i a les dades d'ús a la pàgina web oficial de la Generalitat de Catalunya: https://contractacio.gencat.cat/ca/gestionar-contractacio/contractacio-electronica-administracio/geec/.

El GEEC es va començar a desenvolupar al 2006 arran d'un encàrrec, aprovat per acord del Govern de 05/09/2006, al Departament d'Economia i Finances, a través de la Junta Consultiva de Contractació Administrativa i amb la col·laboració del Centre de Telecomunicacions i Tecnologies de la Informació (CTTI). L'objectiu era la creació de l'eina de tramitació electrònica dels expedients de contractació dels departaments de l'Administració de la Generalitat i dels ens públics que en depenen o hi estan vinculats.

La versió inicial del GEEC va ser aprovada per Ordre ECF/193/2008, de 29 d'abril, i es va desplegar esglaonadament a tots els departaments de la Generalitat i algunes entitats amb gran volum de contractació al 2008.

A l'abril de 2017 es va aprovar l'inici d'una profunda renovació tecnològica del GEEC, que va donar lloc al GEEC 2.0, amb un canvi de tecnologia —es va passar de l'entorn SAP original a una solució web, amb una arquitectura modular basada en microserveis que permet substituir peces de forma independent en cas de necessitat, facilitant l'evolució tecnològica progressiva del sistema—, un entorn més usable, intuïtiu, flexible i escalable, una reducció de costos de desenvolupament, manteniment, implantació i formació, i l'adaptació de l'eina a les modificacions del marc legal derivades de l'entrada en vigor de la LCSP de 2017.

El GEEC 2.0 va ser aprovat per l'Ordre VEH/159/2020, de 21 de setembre, que en regula i descriu les característiques essencials:

a. d'acord amb l'art. 2.1 de l'ordre, és mitjançant el GEEC que «els departaments de l'Administració de la Generalitat i els ens del sector públic que en depenen o s'hi vinculen, **han de tramitar la totalitat de la seva contractació pública**, amb independència de la tipologia d'expedients i dels procediments, formes i instruments utilitzats per a la seva adjudicació», amb l'única exclusió de «les despeses que, per raó de la seva naturalesa i quantia i prèviament autoritzades pels òrgans competents, es tramiten en concepte de manament de pagament a justificar»; el mateix precepte preveu igualment que puguin fer ús del GEEC «els organismes independents i estatutaris que ho sol·licitin»;

b. l'art. 3.2 enumera els **mòduls** de que consta el GEEC, que són els següents:

    i. el «mòdul bàsic de gestió i de seguiment d'expedients», que permet l'inici de l'expedient de contractació per la unitat promotora, la tramitació fins a les fases d'execució, resolució i liquidació del contracte, l'annexió i generació de documents a partir de plantilles preestablertes i personalitzables, la signatura i còpia autèntica dels documents, la visualització de les fases, tràmits i tasques de l'expedient mitjançant un arbre de tramitació interactiu, amb traçabilitat de l'històric d'accions realitzades, la consulta de l'expedient, la generació d'«alertes i avisos sobre el procés de tramitació», l'emissió d'informes operatius, la classificació arxivística dels documents i generació del fitxer d'arxiu de l'expedient, la tramitació excepcional i massiva d'expedients i l'exportació d'informació per ser carregada en quadres de control o eines d'anàlisi d'informació pròpies de les entitats o de la Intervenció General; i

ii. el «mòdul de visor de l'expedient, per a persones no usuàries de l'eina de tramitació que han d'accedir a l'expedient [...] per fer les tasques de generació i fiscalització d'apunts comptables», que permet la cerca d'expedients, la consulta de les dades bàsiques, de tramitació i documentació de l'expedient, i funcions d'exportació d'un expedient per a la seva posterior remissió;

tot això sens perjudici de possibles noves funcionalitats que es puguin anar incorporant, així com d'altres mòduls en funció de noves necessitats que es puguin plantejar;

c. l'art. 2.2 de l'ordre incideix en un element important: **la integració del GEEC amb els sistemes econòmics i financers** corporatius de la Generalitat de Catalunya, i, en aquesta línia, l'art. 4.3 preveu la integració del GEEC amb els sistemes econòmics financers i els quadres de comandament departamentals o propis dels ens públics, i l'art. 4.1 preveu expressament la integració del GEEC amb les aplicacions corporatives de la Generalitat de Catalunya i els sistemes d'informació d'altres administracions vinculats a la contractació pública, fent referència, entre d'altres, als següents:

   i. el sistema econòmic financer corporatiu de la Generalitat de Catalunya (GECAT i Pangea);

   ii. el punt general d'entrada de factures electròniques del Consorci AOC (eFact);

   iii. el Registre públic de contractes (RPC);

   iv. el Registre electrònic d'empreses licitadores i classificades (RELI);

   v. les aplicacions corporatives d'autenticació d'usuaris, de signatura electrònica, de digitalització i còpia autèntica de documents, i de validació de signatures;

   vi. la Plataforma de Serveis de Contractació Pública (PSCP);

   vii. la plataforma d'arxiu de documents electrònics del Consorci AOC (iArxiu);

   viii. l'eina de recepció d'ofertes electròniques (Sobre digital);

   ix. la plataforma de notificacions electròniques (eNotum); i

   x. els sistemes de l'AEAT, la TGSS, l'ATC.

Les dades d'ús del GEEC [38] indiquen una utilització creixent: si al 2020 ho utilitzaven 41 òrgans de contractació, amb 2.692 usuaris, al setembre de 2021 són 52 òrgans de contractació amb 3.054 usuaris.

Paral·lelament, la Generalitat de Catalunya compta amb una altra eina: el **Tramitador electrònic d'expedients de contractació (TEEC)** [39], adreçat a les unitats de contractació del sector públic de la Generalitat i dels ens estatutaris que no disposin del GEEC, així com als ens locals.

[38] Dades actualitzades a setembre 2020. Cfr. nota anterior.

[39] Es pot accedir a informació sobre el TEEC, a la seva normativa reguladora i a les dades d'ús a la pàgina web oficial de la Generalitat de Catalunya: https://contractacio.gencat.cat/ca/gestionar-contractacio/contractacio-electronica-administracio/teec/.

El TEEC va ser aprovat per l'Ordre ECO/295/2015, de 18 de setembre, que, a la seva exposició de motius, ho presenta com «l'eina que ha de facilitar i impulsar la gestió electrònica dels expedients de contractació per a les entitats del sector públic de la Generalitat amb un determinat perfil de contractador que, d'acord amb els criteris objectius d'eficiència, requereixen un sistema d'informació específic i simplificat respecte al que suposa [...] l'eina corporativa del GEEC». El TEEC, que igual que el GEEC 2.0 és una eina d'accés via web, presenta però algunes diferències rellevants respecte del GEEC, que es desprenen de la seva regulació i descripció en la seva esmentada ordre d'aprovació:

a. en primer lloc, tal i com precisa l'art. 1.2 de l'ordre, l'aplicació TEEC «està **basada en productes de mercat**, sobre els quals s'han incorporat funcionalitats a mida [...]. Tot el programari resideix en les instal·lacions del proveïdor de serveis de la Generalitat»;

b. pel que fa a les entitats a les quals va destinada, l'art. 2 distingeix:

    i. per una banda, les «entitats del sector públic de l'Administració de la Generalitat, incloent-hi les universitats catalanes, que [...] no disposin [...] [del GEEC], o no estiguin en disposició d'implementar-la, o que no tinguin una eina de tramitació electrònica de contractes integrable amb els sistemes corporatius de contractació electrònica»; aquestes entitats tenen l'obligació de «tramitar la totalitat dels expedients i processos vinculats a la contractació pública, inclosos els menors, mitjançant el [...] [TEEC], amb independència dels procediments, formes i instruments utilitzats per a la seva adjudicació»; i

    ii. d'altra banda, l'art. 2.1 preveu igualment l'ús del TEEC «per part de les entitats de l'Administració local catalana i els ens, organismes o entitats del seu sector públic i per altres ens, organismes i entitats del sector públic de Catalunya»;

c. l'art. 3.3 de l'ordre descriu detalladament les funcionalitats que ofereix el TEEC, d'entre les quals cal destacar, entre d'altres:

    i. les funcionalitats per a la tramitació d'expedients basada en la gestió d'estats de l'expedient, que determina la informació requerida, la documentació i les validacions exigides, amb possibilitat d'avançar i retrocedir en la tramitació a través de les diverses fases de tramitació —preparació, licitació, adjudicació/formalització i execució—; trobem aquí una diferència rellevant amb el GEEC on la tramitació es basa en fluxos i no en estats, el que representa un nivell més alt d'automatització; el TEEC incorpora un sistema d'avisos; així mateix permet donar d'alta nous circuits de tramitació adaptats a les especificitats de cada entitat a partir dels estats i validacions existents;

    ii. les funcionalitats de gestió documental i d'arxiu, amb incorporació de signatura electrònica dels documents;

    iii. comunicació de la informació al RPC i publicació a la PSCP;

d. finalment, pel que fa a la integració amb altres aplicacions i sistemes, l'art. 4 de l'ordre precisa que està prevista la **integració del TEEC amb les aplicacions corporatives** de la Generalitat de Catalunya següents:

i. els sistemes de control d'accés i d'autenticació d'usuaris, de signatura electrònica, de còpia autèntica de documents, i d'arxiu de de documents electrònics;

ii. el RPC, al qual el TEEC comunica la informació sobre els contractes;

iii. la PSCP per a la publicació d'informació;

iv. el servei de notificacions electròniques eNotum; i

v. «altres serveis corporatius per a la integració amb altres sistemes d'informació a mesura que es produeixen noves necessitats»;

és significatiu el fet que el TEEC no s'integra amb els sistemes d'informació econòmica financera de les entitats usuàries.

Les dades d'ús del TEEC [40] indiquen una utilització més reduïda que el GEEC, en termes d'usuaris i volum de tramitació: mentre que al 2019 es comptaven 98 entitats usuàries, al 2020 eren 97 i al setembre de 2021 són 96 òrgans de contractació amb 401 usuaris.

I pel que fa a sistemes automatitzats d'alerta d'irregularitats, frau o corrupció en la contractació pública, no consta que la Generalitat de Catalunya ni cap dels seus organismes disposi d'aquest tipus de sistemes. La referència de l'art. 3.2 de l'Ordre VEH/159/2020, d'aprovació del GEEC 2.0 a «alertes i avisos sobre el procés de tramitació» s'ha d'entendre en el mateix sentit que la referència de l'art. 3.3 de l'Ordre VEH/159/2020, d'aprovació del TEEC, a «un sistema d'avisos que permet informar de la data límit de presentació d'ofertes, la data de reunions de les meses, la data de devolucions de garanties, etc.».

Cal remarcar, però, que en el seminari web celebrat el 10/03/2021 titulat *Medios electrónicos e inteligencia artificial al servicio de la integridad en la Contratación pública* [41], la subdirectora general de Regulació i Supervisió de la Contractació Pública va manifestar que el desenvolupament d'aquest tipus de sistemes d'alerta era el següent pas en el qual s'estava treballant.

2.3.2 Àmbit local

Per conèixer la situació en l'àmbit local s'ha dut a terme una enquesta entre els ens locals que es podrien considerar amb més recursos i, per tant, en els quals caldria presumir que la digitalització de l'activitat —com a mínim la de contractació pública— està més avançada. S'ha adreçat un qüestionari a un total de 35 ens locals:

a. els ajuntaments de poblacions de Catalunya amb una població de més de 40.000 habitants [42];

[40] Dades actualitzades a setembre 2020. Cfr. nota anterior.

[41] Aquest seminari web es pot veure a: https://www.youtube.com/watch?v=wDz9MT_AeeA&t=215s

[42] Es tracta dels ajuntaments 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 i Vilafranca del Penedès.

b. les quatre Diputacions provincials de Barcelona, Tarragona, Girona i Lleida; i

c. l'Àrea Metropolitana de Barcelona

Les preguntes del qüestionari incidien en els aspectes següents:

a. la solució informàtica de gestió comptable de l'entitat i, en el cas que en tingués, la —o les— de tramitació electrònica d'expedients administratius, distingint entre solucions parcials —només per determinats tràmits del procediment: registre, notificacions, acords i resolucions, etc.— i solucions integrades que suporten la tramitació completa del procediment, així com els àmbits materials en els quals es fa servir la tramitació electrònica —contractació, ajuts i subvencions, autoritzacions i llicències, etc.—;

b. la solució informàtica de tramitació electrònica d'expedients de contractació, en el cas que en tingués, distingint de nou entre solucions parcials i solucions integrades, i demanant igualment si el gestor d'expedients de contractació està integrat amb el sistema d'informació comptable (SIC);

c. si l'ens disposa d'un sistema automatitzat d'alerta en l'àmbit de la contractació pública i, en cas afirmatiu, quines són les alertes concretes que detecta, indicant-ne algunes possibles [43]; i, en cas negatiu, si l'ens té establerts mecanismes no automatitzats de fiscalització i control intern equivalents a un sistema d'alerta i, en aquest cas, quines de les possibles alertes es detecten per aquesta via [42].

Amb un 57,14% de respostes —20 sobre 35 qüestionaris enviats—, els resultats han estat els següents:

a. solució informàtica de tramitació electrònica d'expedients administratius / parcial o integrada:

[43] Les possibles alertes —automatitzades o no— indicades en el qüestionari es referien a:

a. fraccionament;

b. inadequació del procediment per raó de la quantia / de les característiques del contracte;

c. irregularitats en la configuració de la licitació (terminis de presentació d'ofertes; exigències de solvència; criteris d'avaluació; etc.);

d. risc / indicis de vincles entre diversos licitadors;

e. risc / incompliments de solvència de licitadors / prohibicions de contractar;

f. anomalies en les ofertes presentades (oferta única; nombre inesperadament / anormalment baix d'ofertes; nombre inusual d'ofertes inadmissibles; etc.);

g. detecció d'ofertes anormalment baixes;

h. riscos per a la competència per participació en la licitació d'empreses o entitats que han participat en consultes preliminars de mercat;

i. altres (especificar).

Expedient electrònic	Nombre	Percentatge
inexistent	0	0%
integral	15	75%
parcial	5	25%
Total	20	100%

b. àmbits materials d'aplicació de la solució informàtica de tramitació electrònica d'expedients administratius —contractació, ajuts i subvencions, llicències, etc.—:

Àmbits expedient electrònic	Nombre	Percentatge
contractació	20	100%
subvencions	19	95%
autoritzacions	15	75%
altres	7	35%
tots els expedients	9	45%

c. solució informàtica de tramitació electrònica d'expedients de contractació / parcial o integrada / integrada amb SIC:

Contractació electrònica	Nombre	Percentatge
inexistent	0	0%
integral	15	75%
parcial	5	25%
integrada amb SIC	4	20%

d. sistemes automatitzats d'alerta:

Sistema automatitzat d'alerta	Nombre	Percentatge
inexistent	16	80%
fraccionament	2	10%
inadequació procediment	1	5%
irregularitats licitació	1	5%
col·lusió / vincles entre licitadors	1	5%
solvència / requisits per contractar	1	5%
anomalies ofertes	1	5%
ofertes anormalment baixes	2	10%
riscos competència	0	0%
altres	2	10%

e. sistemes no automatitzats d'alerta:

Sistema no automatitzat d'alerta	Nombre	Percentatge
inexistent	3	15%
fraccionament	14	70%
inadequació procediment	17	85%
irregularitats licitació	13	65%
col·lusió / vincles entre licitadors	7	35%
solvència / requisits per contractar	10	50%
anomalies ofertes	11	55%
ofertes anormalment baixes	15	75%
riscos competència	7	35%
altres	4	20%

Aquests resultats, més que una imatge fidel, s'han de considerar una simple aproximació a la situació real. Efectivament, es pot raonablement conjecturar que el grau de digitalització de la part de les entitats que no han contestat el qüestionari —que representen el 42,86% de la mostra seleccionada— és significativament més baix: en aquest sentit resulta revelador que totes les entitats que han contestat manifestin que disposen d'algun tipus de solució informàtica de tramitació electrònica d'expedients administratius.

No obstant, d'aquestes dades podem extreure un parell de conclusions tendencials:

a. d'una banda, es pot afirmar que la contractació electrònica està prou generalitzada en l'àmbit local [44];

b. però, d'altra banda, **la implementació de sistemes automatitzats d'alerta és absolutament excepcional**, malgrat que la majoria d'entitats tenen establerts, a través dels mecanismes fiscalització i control intern, sistemes no automatitzats equivalents a sistemes d'alerta.

[44] En la versió de 2021 de la *Guia per a la contractació electrònica dels ens locals*, elaborada i publicada pel Consorci Localret i accessible a: https://www.localret.cat/guia/nova-versio-2021-de-la-guia-per-a-la-contractacio-electronica-dels-ens-locals/, s'indica, basat en dades del Consorci AOC, que «El 2020 un total de 884 ens locals (d'aquests, 608 ajuntaments) van fer "licitació electrònica" (van utilitzar alguna eina de licitació electrònica):

- 855 ens locals (601 ajuntaments) van fer ús de les eines integrades amb la PSCP: les eines de Sobre Digital i de Presentació Telemàtica d'Ofertes.
- 75 ens locals (33 ajuntaments) van fer ús d'eines de licitació electrònica d'operadores privades.

L'any 2020, el 85% de les licitacions obertes dels ens locals i de les universitats van ser electròniques».

2.3.3 Perspectives

Aquest és doncs el panorama: la datificació de la contractació pública és una realitat bastant estesa, però només de forma ultraminoritària se'n treu profit al servei de la integritat, implementant sistemes automatitzats d'alerta basats en dades.

En aquest context, cal destacar una iniciativa en curs del Consorci Localret que obre unes perspectives prometedores en l'àmbit local. Es tracta d'una consulta preliminar de mercat, realitzada d'acord i a l'empara del que preveu l'art. 115 de la LCSP, per a la preparació d'una futura licitació d'un contracte per dotar els ens locals d'**una eina de seguiment, control i planificació de la contractació**.

La consulta va ser publicada al perfil de contractant del Consorci Localret el 17/05/2021 i l'informe sobre el seu resultat hi va ser publicat el 12/07/2021[45].

L'informe inicial, justificatiu de la conveniència de dur a terme aquesta consulta de mercat, comença exposant que la mateixa pretén donar continuïtat a la presentació, al febrer de 2020, de la *Guia per a la contractació electrònica dels ens locals*, elaborada pel Consorci Localret amb la col·laboració de nombroses institucions de la Generalitat de Catalunya i de l'àmbit local[46], que tenia «l'objectiu principal de delimitar i concretar les principals qüestions que fan referència a la utilització dels mitjans electrònics en la tramitació dels procediments de contractació, incloent propostes i/o recomanacions d'actuació dirigides als òrgans de contractació».

L'informe destaca encertadament, en la línia del que s'ha vingut exposant en el present estudi, que:

> «***L'activitat contractual de les administracions públiques genera un enorme volum de dades, que són públiques*** *—Totes les dades relatives a l'activitat contractual estan publicades, almenys, en el perfil de contractant i en el Registre Públic de Contractes (RPC)—,* ***però que****, amb caràcter general, [les administracions públiques]* ***no poden explotar****, o les exploten amb fulls Excel i/o amb llistats poc àgils.* ***Els mitjans electrònics, informàtics o telemàtics són necessaris per processar (o estructurar) i analitzar aquestes dades****: les administracions públiques necessiten una eina (informàtica) que els permeti estructurar aquestes dades, per tal de poder extreure fàcilment la informació necessària per al seguiment, control i planificació de la contractació».*

Delimitant l'objecte de la consulta, que es concreta en «conèixer si hi ha solucions disponibles al mercat que satisfacin les necessitats dels ens locals de seguiment, control i planificació de la seva contractació, i, si és el cas, preparar

[45] Tota la informació i documentació sobre aquesta consulta preliminar de mercat es troba accessible al perfil de contractant del Consorci Localret, a: https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/notice.pscp?reqCode=viewCtn&idDoc=93133470.

[46] Cfr. nota 44 anterior.

correctament la licitació d'un contracte per dotar-nos d'aquesta solució», l'informe especifica que:

> *«Una eina (o plataforma) informàtica de seguiment, control o supervisió de l'execució i de planificació dels contractes hauria de tenir, almenys, les següents funcionalitats:*
>
> *a) Quadre de comandament que reflecteixi tota l'activitat contractual, que permeti, per exemple, fer amb l'antelació suficient l'avís de pròrroga, o anticipar, si és el cas, la preparació dels nous contractes.*
>
> *b) Espais on les empreses contractistes puguin dipositar la informació necessària per verificar el compliment dels contractes; per exemple, de les clàusules mediambientals, socials, etc.*
>
> *c) Espai de recepció de la prestació, de liquidació del contracte i de gestió de les garanties (ampliació, retorn...).*
>
> *d) Repositori documental de plecs, clàusules, models...»*

La consulta es va instrumentar mitjançant un qüestionari publicat en el perfil de contractant del Consorci Localret que tots els operadors econòmics interessats podien completar i presentar. Les preguntes del qüestionari relatives a les funcionalitats de les diverses solucions feien referència els aspectes següents:

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		

Les dues funcionalitats més interessants als efectes del present informe, evidentment, són les relatives a «alertes automatitzades de finalització dels contractes» —la continuïtat, molt sovint il·legal, de situacions contractuals ja finalitzades és una irregularitat bastant freqüent, especialment en l'àmbit local, que, addicionalment, presenta riscos rellevants de frau i corrupció— i «alertes predefinides». Aquesta última funcionalitat no quedava suficientment concretada en la documentació disponible en el perfil de contractant, tot i que en la presentació que se'n va fer al Congrés Govern Digital [47], es distingien entre

[47] En la taula rodona titulada *Minimitzant els riscos en la contractació pública*, que va tenir lloc, en el marc del Congrés Govern Digital 2021, el 11/11/2021, el cap de l'Àrea de Contractació del

avisos automatitzats de finalització dels contractes i *alertes* referides a fraccionament o a la celebració dels mateixos contractes amb caràcter repetitiu.

L'altre bloc de preguntes del qüestionari que presenta un gran interès als efectes que aquí ens interessen és el referit a l'obtenció de les dades de contractació:

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?
...

L'informe sobre els resultats de la consulta recull els aspectes més rellevants de les respostes de les 5 empreses i entitats que van participar-hi, destacant en primer lloc que:

> *«Les empreses [...] [participants] tenen una solució de seguiment, control i planificació dels contractes. En alguns casos, disposen d'una solució específica; en altres, és un mòdul d'una solució més genèrica de contractació electrònica (que inclou el tramitador o gestor d'expedients i/o l'eina de licitació electrònica, etc.). En aquest segon cas, [...], es tractaria d'un mòdul autònom [...], que, [...], els ajuntaments podrien contractar, sense necessitat d'haver d'adquirir tota la solució completa...».*

Les diverses solucions ofereixen la majoria de les funcionalitats requerides, tot i que es detecten mancances en aquelles relatives a la fase d'execució, recepció i liquidació dels contractes, i, pel que fa específicament a l'obtenció de dades, l'informe indica el següent:

> *«Les **solucions específiques** de seguiment, control i planificació dels contractes; és a dir, aquelles que no s'inclouen dins d'una eina o solució més genèrica de contractació electrònica, **obtenen les dades** (dels contractes) **des de les plataformes públiques de contractació**: PLACE i/o PSCP. En principi les **solucions integrades en una solució genèrica** de contractació electrònica **obtenen aquesta informació directament del tramitador d'expedients o de l'eina de licitació electrònica propis**, però adverteixen que, en el cas que només s'adquirís el mòdul (autònom) de seguiment, aquesta informació es podria obtenir de les plataformes públiques de contractació (PLACE i/o PSCP) o també del Registre Públic de Contractes (RPC), o, si es requerís, del propi gestor d'expedients que tingui l'ajuntament».*

Consorci Localret va presentar aquesta consulta i els seus resultats. Aquesta taula rodona es pot veure a: https://www.youtube.com/watch?v=xCRzrzin24c&list=PLZSCe8AeXET1wLnwFxPIBTDtmG84vUyVj&index=57&t=1466s.

Aquesta distinció és especialment important des de la perspectiva de la disjuntiva entre sistemes d'alerta de caràcter intern o de caràcter extern, que s'abordarà més endavant.

Finalment, cal indicar que el 16/12/2021, el Consorci Localret ha iniciat el procediment per a la conclusió d'un acord marc per a l'adquisició d'una solució informàtica per al seguiment, control i planificació dels contractes públics, amb base en els resultats de l'esmentada consulta preliminar de mercat [48].

A l'apartat 4t del plec de prescripcions tècniques, on es defineixen les funcions de la solució tecnològica objecte de contractació, s'enumeren, entre les «Altres funcionalitats, que inicialment no s'estableixen com a requisits mínims», la d'«**Alertes predefinides de riscos contra la integritat** de la contractació pública: detecció / prevenció d'irregularitats: fraccionaments, celebració dels mateixos contractes amb caràcter repetitiu...».

Tot i que seria desitjable que aquesta funcionalitat no tingués caràcter optatiu, no podem deixar de saludar la incorporació d'aquesta previsió entre els elements que configuren el futur disseny d'aquesta eina.

Nota d'actualització (setembre 2022): el procediment de licitació per a la conclusió de l'acord marc tramitat per Localret va ser resolt per decret de 15/07/2022. No podem deixar de remarcar que l'informe tècnic de valoració de les ofertes segons criteris la quantificació dels quals depèn d'un judici de valor, de 20/06/2022, afirma, tot i que de forma molt succinta, que totes les ofertes presentades incorporaven l'esmentada funcionalitat addicional [50]. Que totes les ofertes incorporin alertes de riscos contra la integritat no deixa de ser significatiu.

[48] Tota la informació i documentació sobre aquesta licitació es troba accessible al perfil de contractant del Consorci Localret: https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/notice.pscp?reqCode=viewCn&idDoc=93360636.

3 Referents

Són nombrosíssims els projectes y les realitzacions que s'han desenvolupat els últims anys de sistemes basats en l'anàlisi de dades per a la detecció i prevenció d'irregularitats, frau i corrupció en l'àmbit de la contractació pública. No tindria sentit intentar fer-ne una enumeració —necessàriament incompleta— ni molt menys una descripció exhaustiva.

Però sí que serà útil fer breument referència i descriure succintament alguns aspectes clau de tres referents que, al nostre entendre, presenten especial interès: l'eina Arachne de la Comissió Europea; el sistema SALER de la Comunitat Valenciana; i el document *Red Flags for Integrity*, publicat per Open Contracting Partnership (OCP).

Per què concretament aquests tres referents?

a. Pel que fa a l'eina Arachne, perquè és la solució tecnològica basada en dades de referència de la Comissió Europea, considerada per aquesta una bona eina de lluita antifrau; la seva importància com a solució ja existent, a la qual es pot adherir tota administració gestora o beneficiària dels fons NextGenerationEU, és doncs evident.

b. El sistema SALER de la Comunitat Valenciana va ser pioner en l'àmbit que aquí ens ocupa, i el marc legal en el qual es fonamenta i que li dona cobertura normativa resulta de gran interès.

c. Finalment, el document *Red Flags for Integrity* de OCP es pot considerar una referència inexcusable que no només ofereix valuoses orientacions metodològiques tant per la implantació com pels dissenys de sistemes d'alerta basats en dades, sinó que igualment inclou un annex que, en la seva última versió, actualitzada a maig de 2021, ofereix un llistat detallat de 73 possibles alertes definides amb base en l'estàndard de dades de contractació pública OCDS dissenyat per OCP.

3.1 Eina Arachne

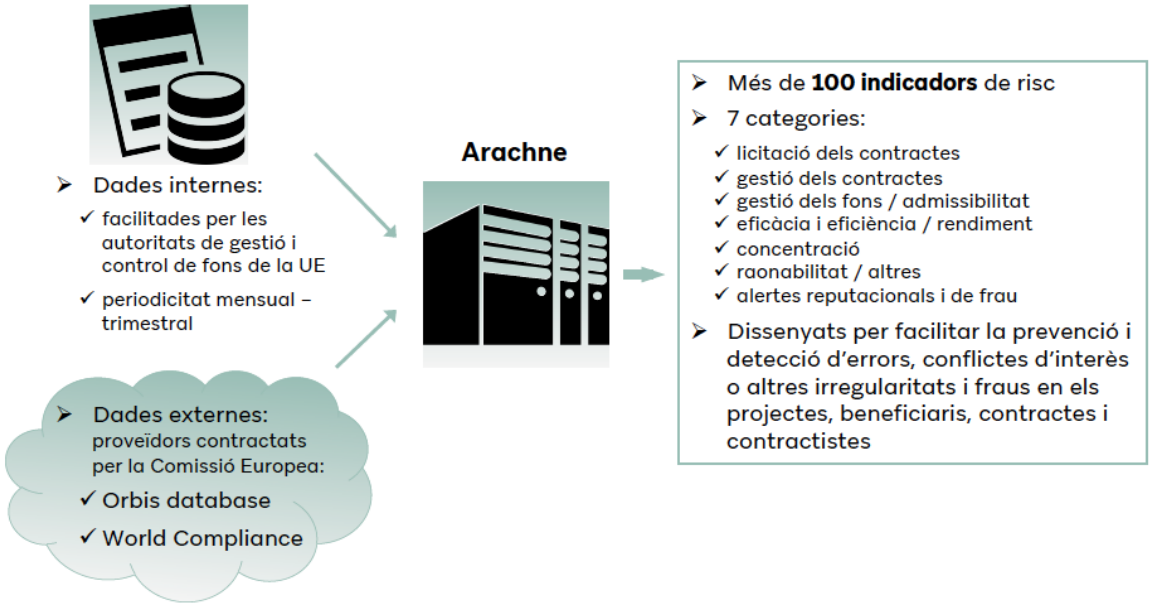
Com ja hem apuntat [49], Arachne és una **eina tecnològica integrada de mineria i enriquiment de dades**, desenvolupada per la Comissió Europea des de 2009 i plenament operacional des de setembre de 2015, i **posada gratuïtament a**

[49] Cfr. nota 4 anterior. Es pot trobar àmplia informació sobre l'eina Arachne a la web oficial de la Comissió Europea: https://ec.europa.eu/social/main.jsp?catId=325&intPageId=3587&langId=es#navItem-relatedLinks, que conté enllaços a diversos documents de gran interès, especialment la presentació i el document de preguntes freqüents (únicament disponibles en anglès), accessibles, respectivament, en: https://ec.europa.eu/social/main.jsp?catId=738&langId=en&pubId=7883&type=2&furtherPubs=yes (presentació), i a: https://ec.europa.eu/social/BlobServlet?docId=15097&langId=en (preguntes freqüents).

disposició dels Estats membres de la UE[50] per tal de donar suport a les autoritats de gestió i de control dels fons europeus en la seva activitat administrativa i de control per **prevenir i detectar errors i irregularitats en els projectes, beneficiaris, contractes i contractants**.

Recordem en efecte[51] que l'art. 125.4 c) del Reglament (UE) 1303/2013, del Parlament Europeu i del Consell, de 17 de desembre de 2013, sobre disposicions comunes relatives als fons europeus, estableix l'obligació d'«aplicar mesures antifrau eficaces i proporcionades, tenint en compte els riscos detectats» en la gestió d'aquells fons; doncs bé, en relació amb el compliment d'aquesta obligació la utilització d'Arachne, com a mesura antifrau basada en dades, és considerada el referent per la Comissió[52].

El funcionament de l'eina Arachne és el següent: a partir de dades internes, facilitades pels propis ens gestors i de control dels fons europeus, enriquides amb dades externes, facilitades per dos proveïdors externs, el sistema ofereix fins a 106 indicadors classificats en 7 categories: licitació i adjudicació dels contractes, gestió dels contractes, gestió dels fons (admissibilitat de despeses), rendiment (eficàcia i eficiència en l'ús dels fons), concentració, raonabilitat i alertes reputacionals i de frau. Esquemàticament aquest funcionament es podria representar de la manera següent:



[50] La *Carta per a la introducció i aplicació de l'eina Arachne d'avaluació del risc en les verificacions de la gestió*, accessible a: https://ec.europa.eu/social/BlobServlet?docId=14836&langId=es, estableix un conjunt de principis comuns que tant les autoritats de gestió de fons europeus com els serveis de la Comissió s'han de comprometre a respectar per a l'adopció, aplicació i integració de l'eina Arachne d'avaluació de riscos en els procediments de verificació de la gestió dels fons.

[51] Cfr. nota 34 anterior.

[52] En el document de preguntes freqüents s'especifica que «Arachne no és d'ús obligatori i per tant opcional. Les autoritats de gestió han d'implementar mesures antifrau efectives i proporcionades d'acord amb l'article 125 (4) (c) del Reglament (EC) 1303/2013 i Arachne pot representar un element complementari d'aquestes mesures. Arachne és considerada una bona pràctica per la comissió».

Repassem breument cadascun dels diferents elements que integren aquest sistema.

3.1.1 Dades internes

L'art. 72 d) del Reglament (UE) 1303/2013 imposa als beneficiaris i gestors de fons europeus l'obligació de «comptar amb sistemes informàtics per a la comptabilitat, per a l'emmagatzematge i la transmissió de les dades financeres i les dades sobre indicadors i per al seguiment i l'elaboració d'informes». Aquests sistemes informàtics són la font de les **dades internes** que utilitza l'eina Arachne.

En efecte, les organitzacions i entitats usuàries tenen l'obligació de transmetre regularment —idealment amb periodicitat mensual i, com a mínim, trimestralment; l'incompliment d'aquesta obligació pot comportar la retirada de l'accés a l'eina Arachne—, en format XML, extraient-les dels seus propis sistemes informàtics i carregant-les en un servidor específic de la Comissió Europea, les referides dades internes per a la gestió dels fons [53]: projectes, beneficiaris, contractes, contractistes i despeses.

Totes aquestes dades internes es conserven en el sistema Arachne durant un temps limitat, determinat per la normativa sobre gestió de fons europeus —fins a un màxim de 3 anys després de l'aprovació per la Comissió dels comptes anuals de cada programa operatiu per a la programació 2014-2020—.

3.1.2 Dades externes

L'eina Arachne creua i enriqueix les dades internes amb **dades externes** facilitades per dos proveïdors externs contractats per la Comissió Europea:

a. Bureau Van Dijk, que facilita la informació de la seva base de dades **Orbis database**, amb dades financeres (volum de negoci, flux de caixa, beneficis, etc.) i informació sobre accionistes, filials, seu social, tipus i mida d'empresa, sector d'activitat, representants oficials i d'altres indicadors de credibilitat i solvència de més de 200 milions d'empreses de tot el mon; i

b. LexisNexis, que aporta la base de dades **World Compliance**, amb llistats de persones políticament exposades (PEP) —persones que ocupen càrrecs públics especialment susceptibles de trobar-se amb situacions de conflicte d'interès—, persones i entitats sancionades i vinculades a activitats delictives (tràfic de drogues o de persones, blanqueig de capitals, frau fiscal o financer, etc.) així com informacions adverses en els mitjans de comunicació.

[53] Les dades mínimes a transmetre són les especificades a l'annex III del Reglament delegat (UE) 480/2014 de la Comissió, de 3 de març de 2014, que desenvolupa el Reglament (UE) 1303/2013. No obstant, amb aquestes dades mínimes, Arachne no pot calcular tots els indicadors possibles. Les autoritats beneficiàries i gestores dels fons poden, amb caràcter voluntari, ampliar el nombre de camps de dades transmesos al sistema Arachne, per poder disposar de més informació i indicadors generats per Arachne. Per això la Comissió recomana incloure en els sistemes informàtics de gestió dels fons europeus tots els camps de dades susceptibles de ser transmesos a Arachne per al seu processament, per tal de poder beneficiar-se de tot el seu potencial.

Aquests proveïdors externs de dades van ser seleccionats per la Comissió Europea [54] després d'un estudi de mercat, basant-se especialment en el fet que les dades de dues bases de dades esmentades provenien de fonts oficials d'accés públic [55] i no de fonts no oficials o poc fiables. Addicionalment és responsabilitat d'aquests dos proveïdors externs garantir la qualitat i la fiabilitat de les dades facilitades.

Les dades externes són actualitzades amb periodicitat trimestral.

Per últim cal remarcar, en relació amb el tractament per Arachne tant de les dades internes com externes, des del punt de vista del règim legal de protecció de dades, que la Comissió Europea va presentar davant del Supervisor Europeu de Protecció de Dades la notificació corresponent obtenint un dictamen favorable sobre el compliment per Arachne de les disposicions del Reglament (CE) 45/2001 del Parlament Europeu i del Consell, de 18 de desembre 2000, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals per les institucions i els organismes comunitaris i a la lliure circulació d'aquestes dades —actualment derogat i substituït pel Reglament (UE) 2018/1725 del Parlament Europeu i del Consell, del 23 d'octubre de 2018—. Per la seva banda, les autoritats nacionals usuàries d'Arachne han de complir igualment les normes nacionals i europees en matèria de protecció de dades, el que implica, entre d'altres conseqüències, que les dades i indicadors de riscos facilitats per Arachne no poden ser publicats.

3.1.3 Indicadors generats per Arachne

A partir de les dades internes i externes, Arachne genera 106 indicadors classificats en 7 grans categories [56]:

a. contractació pública: 6 indicadors referits als procediments de licitació i adjudicació dels contractes finançats amb fons europeus;

b. gestió dels contractes: 10 indicadors relatius a la gestió de l'execució dels contractes en funció de les dades comparatives amb contractes de característiques anàlogues;

c. admissibilitat de despeses: 14 indicadors per a la gestió dels fons, que permeten verificar l'admissibilitat de les despeses a finançar tant des del punt de vista temporal com material;

[54] La Comissió Europea va concloure un contracte marc amb una durada que cobreix el termini de finalització de la programació 2014-2020. Està prevista una avaluació de l'impacte i la utilitat de l'eina Arachne que determinarà, en funció de les disponibilitats pressupostàries, l'eventual renovació del contracte per tal de continuar garantint la gratuïtat de la utilització d'Arachne per les autoritats nacionals.

[55] Les dades sobre sancions i persones o entitats sancionades són objecte de tractament de conformitat amb allò que disposa l'art. 11 del Reglament (UE) 2018/1725 del Parlament Europeu i del Consell, del 23 d'octubre de 2018, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals per les institucions, òrgans i organismes de la Unió, i a la lliure circulació d'aquestes dades.

[56] Aquesta descripció es basa en el document de la Comissió Europea *Arachne. What is new in Arachne v2.0*, de 16/02/2017, accessible en l'enllaç indicat en la nota 49 anterior.

d. rendiment: 18 indicadors d'eficàcia i eficiència en la utilització dels fons, que permeten avaluar la coherència de l'activitat subvencionada en funció dels referents sectorials;

e. concentració: 13 indicadors dissenyats per facilitar la detecció de concentracions de fons europeus en els mateixos beneficiaris, mitjançant el creuament de dades a nivell de projectes i programes;

f. altres: 16 indicadors bàsics sobre coherència i raonabilitat dels projectes; i

g. alertes reputacionals i de frau: 30 indicadors que cobreixen els 5 àmbits de risc següents:

    i. riscos financers: 6 indicadors de la situació financera dels beneficiaris i participants en els projectes, contractistes i subcontractistes i integrants d'unions d'empreses, basats en dades financeres;

    ii. riscos de vinculacions: 7 indicadors referits l'existència de possibles vinculacions entre els beneficiaris i participants en els projectes, contractistes i subcontractistes i integrants d'unions d'empreses;

    iii. riscos reputacionals: 6 indicadors sobre participació en activitats que puguin comportar un perjudici reputacional;

    iv. sancions: 4 indicadors de l'aparició dels beneficiaris i participants en els projectes, contractistes i subcontractistes i integrants d'unions d'empreses en qualsevol tipus de llistes d'entitats sancionades o en situació de prohibició de contractar;

    v. canvis: 6 indicadors de canvis en l'estructura de les empreses o entitats.

Cal precisar que un valor alt de risc indicat en un indicador concret no es pot considerar de cap manera una prova de l'existència d'una irregularitat de qualsevol mena. En aquest sentit, Arachne s'ha de considerar un sistema d'*alerta*, que, mitjançant la informació que genera, indica la *possible o potencial* existència d'alguna irregularitat, el que —en teoria— hauria de donar lloc a la corresponent verificació o investigació per confirmar o descartar-ne l'existència efectiva.

Resulta especialment interessant que Arachne permeti igualment a les autoritats nacionals introduir en el sistema les dades de les persones que en formen part involucrades en la gestió i control dels fons europeus, sempre, evidentment, dins del respecte de les disposicions nacionals i europees en matèria de protecció de dades.

Els indicadors generats per Arachne faciliten informació, en termes de nivells de risc referits als diversos beneficiaris, contractistes i subcontractistes, útil en les diverses fases de la gestió dels fons. Així:

a. en les fases de selecció dels beneficiaris i adjudicació dels contractes els indicadors permeten detectar els riscos vinculats a situacions de conflicte d'interès, d'incompliment de les normes europees sobre ajudes d'estat o de manca de capacitat administrativa o de solvència, entre d'altres;

b. en les fases d'execució dels projectes els indicador faciliten alertes sobre riscos d'errors o irregularitats en la contractació i execució de contractes, admissibilitat de despeses, concentració de fons en els mateixos beneficiaris, baixos rendiments o inconsistències en els projectes; i

c. en la fase final d'autoria i avaluació dels projectes conclosos, els indicadors permeten avaluar els impactes positius dels mateixos.

No obstant, cal puntualitzar igualment que els indicadors d'Arachne també presenten algunes limitacions. Així, per exemple, no permeten detectar situacions de col·lusió entre licitadors, ni l'acumulació en un mateix beneficiari de fons europeus i d'altres tipus de subvencions incompatibles. I, pel que fa a la detecció dels conflictes d'interès, Arachne només pot detectar vinculacions de naturalesa jurídica, corresponent al fet d'ocupar formalment càrrecs o llocs en les diverses entitats analitzades; l'existència del que es podria denominar **vinculacions privades o difuses** —relacions de negocis, familiars, d'amistat, o altres anàlogues— no són susceptibles de ser detectades per l'eina Arachne. Aquesta és una limitació que el sistema SALER aspira a superar.

3.2 Sistema SALER

El sistema SALER, és un projecte pioner de la Generalitat Valenciana que, pel que fa a la seva implementació operativa es troba en desenvolupament constant, i del qual resulta d'un gran interès el **disseny a nivell normatiu**, establert a la Llei 22/2018, de 6 de novembre, de la Generalitat, d'Inspecció General de Serveis i del sistema d'alertes per a la prevenció de males pràctiques en l'Administració de la Generalitat i el seu sector públic instrumental.

De fet, és el primer intent d'aplicar el plantejament que es defensa en aquest estudi: **treure profit de la datificació de l'activitat del sector públic al servei de la integritat**, implementant sistemes automatitzats d'alerta basats en dades. Així ho explicita l'exposició de motius de la Llei 22/2018 que afirma les següents premisses sobre les quals es fonamenta el disseny del sistema:

> *«La sofisticació cada vegada major dels processos d'obtenció, emmagatzematge i anàlisi de dades representa una important oportunitat per a la prevenció d'irregularitats i males pràctiques. […] resulta factible* ***aprofitar les possibilitats que ofereix l'anàlisi de dades per a enriquir de manera significativa el procés d'avaluació del risc****. Així,* ***mitjançant la utilització i interconnexió de les dades amb les quals compta l'administració pública resulta possible detectar probables situacions de risc, fins i tot abans que s'acaben produint irregularitats****. […]*
>
> *… aquesta llei garanteix el correcte maneig d'una eina de prospecció de dades, el sistema d'alertes ràpides, per a identificar els processos administratius que poden ser susceptibles de presentar risc d'irregularitats o males pràctiques. Aquest sistema és un instrument de classificació i identificació del risc que va dirigit a reforçar la identificació, prevenció i detecció primerenca d'aquestes pràctiques en els processos administratius de gestió. […]*

Aquest sistema d'alertes, juntament amb l'elaboració d'un mapa d'avaluació de riscos, els plans individuals d'autoavaluació i la publicació d'un codi de bones pràctiques per a la prevenció i detecció d'irregularitats, constituiran els instruments bàsics de caràcter preventiu que permetran reduir els riscos d'irregularitats o males pràctiques administratives.»

Existeix poca informació o documentació publicada sobre el sistema SALER i per això resulta d'allò més interessant un article publicat a l'octubre de 2019 per Alfonso PUNCEL CHORNET, subsecretari de la Conselleria de Transparència del Govern valencià entre juliol de 2015 i juliol de 2019 i, com a tal, responsable de la Inspecció General de Serveis (IGS) i del disseny i desenvolupament del sistema SALER, on es detallen els antecedents i les circumstàncies de la concepció del sistema, i se'n detallen a nivell general i introductori els aspectes principals [57].

En l'esmentat article es destaquen especialment els reptes als quals es va haver de fer front en la concepció i el disseny del sistema SALER, el primer dels quals era, precisament, la manca de cap referent preexistent:

«... 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».*

Efectivament, el sistema SALER no limita el seu àmbit d'aplicació a la contractació pública, sinó que aspira a «obtenir alertes sobre males pràctiques en diferents processos de gestió (contractació, utilització del patrimoni públic, selecció de personal, incompatibilitats, concessió d'ajuts, subvencions, etc.)» [58]. D'altres reptes van sorgir a l'hora de possibilitar l'accés a les dades per part de la IGS, responsable i gestora del sistema SALER, així com en fer front a les dinàmiques i resistències al canvi de l'administració [59].

---

[57] Article *Inteligencia artificial para la transparencia pública. El Sistema de Alertas Tempranas* (SALER) de la Generalitat Valenciana, publicat al núm. 3116, d'octubre de 2019 del Boletín Económico del ICE, pàg. 41 a 61; accessible a: http://www.revistasice.com/index.php/BICE/article/view/6914/6928.

[58] Op. cit. pàg. 45. Cfr. nota anterior.

[59] Op. cit. pàg. 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»; pàg. 51: «... 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 57 anterior.

Però el repte principal va ser **transformar el coneixement administratiu sobre riscos de possibles males pràctiques i irregularitats en els algoritmes que, a partir de les dades disponibles, generin les alertes** corresponents.

En paraules de PUNCEL CHORNET: «... el veritable "cor" del projecte [...] es troba en el coneixement administratiu i en la part creativa de definir riscos, alertes, algoritmes, [...]. De fet, la part més complexa era definir, per a cada àmbit de gestió, els indicadors i els patrons de normalitat que ens permetessin disposar d'alertes cada vegada més precises i efectives», és a dir: «establir patrons de comportament "normal" i determinar aquells comportaments que s'aparten de dits patrons predefinits com a normals i que podrien ser indicatius de males pràctiques o irregularitats».

La descripció general del funcionament del sistema SALER és, segons PUNCEL CHORNET, la següent:

> *«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 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 translació i el desenvolupament d'aquesta idea en seu normativa es troba en el capítol I, titulat precisament *Sistema d'alertes*, del títol II de la Llei 22/2018, que inclou dues seccions:

a. la primera, *Elements del sistema d'alertes, adscripció i instruments de gestió del risc* —arts. 17 a 24—, que conté la definició i descripció del diversos elements que integren el sistema d'alertes; i

b. la segona, *Característiques tècniques i funcionalitats del sistema* —arts. 25 a 29—, més centrada en aspectes relatius al funcionament operatiu del sistema: la compatibilitat, desenvolupament, explotació i manteniment del sistema informàtic; les garanties de seguretat del sistema; la classificació de riscos i codificació de resultats de les actuacions d'investigació de la IGS; el codi de bones pràctiques i els protocols d'actuació; i les previsions d'avaluació periòdica del sistema.

Així, l'art. 17 de la Llei comença, en el seu apartat 1r, descrivint el sistema SALER indicant que «… s'articularà mitjançant un conjunt d'eines la interacció de les quals permet la detecció de possibles irregularitats i males pràctiques administratives, amb caràcter preventiu, a partir de l'anàlisi de la informació obtinguda i de l'avaluació de factors de risc que potencialment puguin originar-les».

A partir d'aquesta definició general, els següents preceptes de la llei descriuen minuciosament els diversos **elements que integren el sistema SALER**, que, d'acord amb l'art. 17.2 de la Llei 22/2018, són els següents:

a. les **dades** —art. 17.2 a)—, provinent tant de bases de dades pròpies de la Generalitat valenciana —art. 18 de la Llei— com d'altres organismes o entitats —art. 19— i, igualment —i això és especialment interessant— obtingudes de fonts obertes, particularment d'Internet —art. 17.3; de seguida tornarem amb més detall sobre aquest aspecte—;

b. el **sistema lògic i informàtic de processament de dades** —art. 17.2 b)—, constituït, segons estableix l'art. 20 de la Llei, per «El conjunt d'eines de programari i la infraestructura de servidors i bases de dades amb què funcionen», «El conjunt de dades obtingudes mitjançant processos d'extracció, transformació i càrrega a partir de la informació continguda en les bases de dades» i «Els mecanismes d'anàlisi de dades que, a través d'indicadors de risc definits per a cadascun dels diferents àmbits de gestió administrativa sobre els quals actuarà el sistema, permeten la detecció de situacions irregulars susceptibles d'investigació»;

c. les **avaluacions**, el **mapa d'avaluació de riscos** i les **autoavaluacions individuals** —art. 17.2 c)—, regulats, respectivament, als arts. 21, 22 i 23 de la Llei; i

d. els **informes de conclusions i recomanacions** de cada actuació d'investigació de la IGS i també els **informes d'avaluació del propi sistema** SALER que ho retroalimenten —art. 17.2 d)—.

Com acabem de veure, les dades que fa servir el sistema no només provenen de bases de dades internes de la Generalitat valenciana i del seu sector públic instrumental, o d'altres organismes i entitats, sinó també de fonts obertes. Aquest és un aspectes especialment interessant del sistema SALER, amb el qual aspira a superar alguna de les limitacions ja apuntades de l'eina Arachne. Aquesta possibilitat planteja, però, qüestions rellevants des del punt de vista de la protecció de dades personals. I a aquest respecte l'exposició de motius de la Llei destaca el següent:

> *«La posada en marxa del sistema d'alertes […] comporta el **tractament de dades personals de persones físiques** que resulten rellevants per al compliment dels seus fins, sempre respectant els seus drets, especialment els fonamentals, […]. Les dades a tractar se circumscriuen a les persones que mantinguin, o hagin mantingut, qualsevol relació jurídica amb l'administració de la Generalitat, […].*
>
> *Les dades poden procedir de tres fonts: bases de dades internes creades i mantingudes per l'administració de la Generalitat i el seu sector públic*

instrumental amb les dades que els interessats han proporcionat voluntàriament per a la tramitació del procediment a través del qual s'han relacionat amb l'administració; bases de dades d'organismes o entitats externes amb què s'estableixi una col·laboració, per exemple registres públics; i, finalment, ***dades de caràcter personal que els seus titulars hagin fet manifestament públiques****, particularment en internet.*

Respecte a l'últim grup de dades, ha d'aclarir-se que el seu tractament es limita exclusivament a aquelles dades que resulten rellevants per al desenvolupament d'una investigació en la mesura que puguin permetre detectar signes externs d'un nivell adquisitiu desproporcionat, relacions entre els interessats o entre aquests i el personal al servei de l'administració pública o el seu sector públic instrumental, per exemple.»

Tot i així, l'exposició de motius de la llei afirma la compatibilitat de les seves previsions amb les disposició del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (RGPD), precisant que el tractament de les dades personals dut a terme pel sistema SALER s'empara en l'art. 6 c) i e) del RGPD —tractament per al compliment d'una obligació legal i/o per al compliment d'una missió d'interès públic o en l'exercici de poders públics—.

Aquestes cauteles i prevencions en matèria de protecció de dades s'observen molt clarament en la regulació, a l'art. 17.3 de la Llei, relatiu a les dades personals obtingudes de fonts obertes, que disposa el següent:

«També es podran integrar en el sistema dades personals de persones o entitats que tinguin o hagin tingut una relació directa amb l'administració de la Generalitat i el seu sector públic instrumental referides a expedients administratius relacionats amb la contractació, amb ajudes o subvencions públiques, així com de les persones o entitats que mantinguin o hagin mantingut una relació laboral o contractual amb l'administració de la Generalitat i el seu sector públic instrumental.

Per a les finalitats previstes en aquesta llei podran tractar-se les ***dades que els interessats*** *descrits en el paràgraf anterior* ***hagin fet manifestament públiques de manera voluntària, particularment en internet****.*

Per a això, hauran de reunir-se les condicions següents:

*a) Que aquests espais tinguin la condició d'****oberts*** *i* ***no estiguin protegits pel dret a la intimitat o el dret al secret de les comunicacions****.*

b) Que, en el cas de xarxes socials, es tracti de pàgines indexables per cercadors, espais oberts a tots els membres de la xarxa, xarxes socials obertes o xarxes la naturalesa professional, empresarial o similar de les quals ***permeten excloure tota expectativa de privacitat****.*

*c) Que **en cap cas siguin objecte de tractament les dades de terceres persones** relacionades amb els investigats.»*

Aquestes previsions es completen amb una **explícita regulació del termini de conservació de les dades** i de les **limitacions als drets reconeguts pel RGPD**. L'exposició de motius de la Llei precisa que «atès que l'exercici de males pràctiques i irregularitats moltes vegades només pot detectar-se si s'analitzen les dades acumulades en un període de temps, resulta imprescindible per al compliment dels fins del sistema que la llei, d'acord amb les possibilitats que ofereix el reglament europeu, reguli dos aspectes fonamentals que tenen incidència directa sobre aquesta capacitat d'anàlisi: un termini ampli de conservació de les dades, que se situa en vuit anys, i la limitació dels drets regulats en els articles 12 a 22 del reglament».

La Llei 22/2018 entrava en vigor, d'acord amb la seva disp. final 2a, als 20 dies de la seva publicació al DOGV, que va tenir lloc el 08/11/2018, però el 2n incís de l'esmentada disp. final 2a preveia que les previsions relatives al sistema SALER entrarien en vigor en el moment en que es determinés pel conseller o consellera responsable de la IGC, dins d'un termini màxim de 6 mesos des de la publicació de la llei. Aquesta previsió es va complir mitjançant resolució de 31/01/2019 del conseller de Transparència, Responsabilitat Social, Participació i Cooperació, publicada al DOGV el 07/02/2019.

Hem vist que un dels reptes principals en el disseny i implementació del sistema SALER va ser precisament convertir, a partir del coneixement administratiu sobre possibles riscos, les dades en alertes, mitjançant els algoritmes corresponents. Doncs bé, per aquesta tasca, resulta extremadament útil l'estudi *Red Flags for Integrity* publicat per OCP el 2016.

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

Open Contracting Partnership és una col·laboració «entre governs, empreses, la societat civil i especialistes en tecnologia per fer transparent i transformar la contractació pública a tot el món», creada inicialment pel Banc Mundial i establerta el 2015 com a programa independent sense ànim de lucre, patrocinat pel Fund for the City of New York (Fons per a la Ciutat de Nova York)[60].

OCP ha dut a terme nombrosos projectes, però als efectes d'aquest estudi, dos són d'especial interès:

a. l'Estàndard de Dades de les Contractacions Obertes (OCDS, per l'acrònim de la denominació oficial en anglès: *Open Contracting Data Standard*); i

b. el ja esmentat document *Red Flags for Integrity: Giving the green light to open data solutions* (Banderes vermelles per la integritat: llum verda a les solucions basades en dades obertes), publicat per OCP el 2016.

L'OCDS és un estàndard de dades obertes de contractació pública que «permet la divulgació de dades i documents en totes les etapes del procés de

[60] Informació sobre OCP en la seva pàgina web oficial, accessible a: https://www.open-contracting.org/es/about/.

contractació mitjançant un model de dades comú» i va ser creat «per ajudar les organitzacions a augmentar la transparència de la contractació i permetre una anàlisi més profunda de les dades contractació per part d'una àmplia gama d'usuaris», tal i com s'indica a la web oficial corresponent [61].

Per la seva part, el document *Red Flags for Integrity* és una publicació d'OCP de novembre de 2016 que consta de dos documents:

a. el document *Red Flags for Integrity* pròpiament dit, que constitueix una guia metodològica molt pràctica per al disseny i implementació d'un sistema d'alerta en l'àmbit de la contractació pública; i

b. el document complementari *Red Flags to OCDS Mapping*, en format de full de càlcul, que, en la seva versió més recent, de maig de 2021, conté un llistat de 73 possibles alertes —el document utilitza el terme *red flag* (bandera vermella), d'ús habitual a nivell internacional; utilitzarem la traducció: *alerta*—, detalladament definides majoritàriament a partir de les dades del model OCDS; tal com s'indica en el propi document, aquesta nova versió del llistat és el resultat de depurar el llistat originari de 2016 —amb 119 possibles alertes— eliminant duplicitats i algunes alertes basades en dades no incloses en el model OCDS, i d'afegir-hi noves alertes; així mateix, la nova versió inclou el detall de les dades del model OCDS necessàries per a cada alerta, el mètode de càlcul aplicat, la descripció i l'explicació de l'alerta i els documents de referència —publicacions acadèmiques o d'investigació— en els quals es basa cada alerta [62].

No té, evidentment, sentit reproduir aquí el document en qüestió, però val la pena remarcar especialment algunes reflexions i consideracions metodològiques, especialment encertades i útils, contingudes en el mateix.

3.3.1 Interès i utilitat dels sistemes d'alerta

La primera idea en la qual incideix el document és l'**enorme potencial dels sistemes d'alerta basats en l'anàlisi de dades en temps real**, en la mesura en que permeten detectar les possibles irregularitats i els riscos potencials de frau i

[61] Tota la informació disponible sobre l'OCDS es troba en anglès (versió oficial de referència), francès i castellà en la web oficial: https://standard.open-contracting.org/latest/es/.

La informació disponible en aquesta web inclou una presentació i introducció general al OCDS, una guia per al disseny i implantació de l'OCDS en qualsevol organització, la definició detallada del model de dades i les regles d'aplicació corresponents, eines d'ajuda i indicacions per a l'obtenció d'ajuda per a la implantació de l'OCDS, l'històric de l'estàndard OCDS i una eina de revisió de dades per a la verificació de la correcta implantació d'aquest model de dades obertes de contractació pública.

[62] Tant el document *Red Flags for Integrity* com el document complementari *Red Flags to OCDS Mapping*, es troben en la pàgina oficial d'OCP, accessibles, lamentablement **només en anglès**, a: https://www.open-contracting.org/es/resources/red-flags-integrity-giving-green-light-open-data-solutions/.

Es pot trobar més informació sobre el document, els seus objectius i els experts que van participar en la seva elaboració, entre d'altres, en la publicació de 30/11/2016 del blog d'OCP accessible a: https://www.open-contracting.org/es/2016/11/30/red-flags-integrity-giving-green-light-open-data-solutions/.

corrupció abans que s'hagi consumat la seva producció i s'hagin verificat els riscos [63].

En aquest sentit, el document remarca especialment com es constata l'evolució en els estudis sobre corrupció des d'una perspectiva reactiva i punitiva cap a noves aproximacions centrades en el control de la contractació mitjançant **sistemes d'alerta**, insistint en el seu **caràcter intrínsecament proactiu** [64], i destacant com aquests sistemes s'alineen amb els plantejaments del document *Principis de dades obertes anticorrupció* aprovat pel G20 i de la *Carta internacional de Dades Obertes*, als quals ja hem fet referència [65].

Així mateix, el document incideix en una idea ja apuntada —en tractar l'eina Arachne; cfr. apartat 3.1.3 anterior—: que, en general, els indicadors d'alerta no s'han de considerar proves concloents d'irregularitats, frau o corrupció, sinó només indicis de l'existència d'un fet o una circumstància anòmala, que justifica una revisió o investigació més acurada.

3.3.2 Idees clau

Des d'una perspectiva conceptual, cal destacar 3 idees clau del document que ens ocupa que, com precisa en la seva introducció, pretén donar resposta a dues qüestions essencials: quines dades són necessàries per a la detecció de les irregularitats, el frau i la corrupció, i com es poden fer servir i per què.

Primera idea: la **importància del context**. Diversos estudis generals demostren que, amb caràcter general, les irregularitats i els comportaments constitutius de frau o de corrupció en la contractació pública es poden reconduir a 4 grans categories o esquemes il·lícits [66]. Això fa que les diverses alertes siguin

[63] *Op. cit.* pàg. 4: «Una de les promeses més interessants de l'anàlisi de dades en temps real en contractació pública és que la corrupció el frau poden potencialment ser detectats i previnguts abans d'ocórrer, en lloc de deixar que els poders públic endrecin les destrosses *a posteriori*».

[64] *Op. cit.* pàg. 6: «Pot ser també més efectiu centrar-se en desenvolupar plantejaments proactius més que reactius per al control de la contractació pública, mitjançant sistemes d'alerta. […] Des d'aquest punt de vista, els sistemes d'alerta són una eina proactiva, i no merament reactiva».

[65] Cfr. apartat 2.1.2 anterior (pàg. 17 i 18) i notes 16 i 17.

[66] El document *Red Flags for Integrity* fonamenta aquesta afirmació principalment en la *Guia per la lluita contra la corrupció i el frau en els projectes de desenvolupament* (*Guide to Combating Corruption & Fraud in Development Projects*) —accessible (en anglès) a: https://guide.iacrc.org—, elaborada pel Centre Internacional de Recursos Anticorrupció (International Anti-Corruption Resource Center) —web oficial: https://iacrc.org—, així com als treballs en els quals es fonamenta el projecte *DIGIWHIST, The Digital Whistleblower* —cfr. nota 2 anterior—.

Les 4 grans categories serien les següents:

a. la corrupció pròpiament dita, que inclouria el suborns i comissions i els interessos ocults;

b. la manipulació de licitacions, que inclouria diverses tipologies d'irregularitats amb incidència en el procés de licitació —irregularitats en la informació sobre la licitació, en la definició de les especificacions i requisits, en la selecció dels licitadors, en els criteris d'adjudicació, en la formació de les ofertes, fraccionament, etc.—;

c. la col·lusió entre licitadors; i

homologables i aplicables, a nivell conceptual, en diversos països i contexts, en la mesura que l'esquema il·lícit subjacent és el mateix. Això no obstant, és absolutament necessari, per tal que les alertes concretament dissenyades operin de forma eficient i eficaç, **contextualitzar el disseny general adaptant-ho a les singularitats de cada marc legal i context social i econòmic**. Aquesta adaptació al context concret en el qual ha d'operar l'alerta és especialment important per tal d'evitar falsos positius: alertes que no corresponen a cap irregularitat real ni potencial, provocades per deficiències en la definició dels valors llindars de les dades utilitzades que fan saltar l'alerta.

Segona idea: conveniència d'utilitzar una **estratègia de "triangulació"**, entesa com la **utilització agregada de més d'una dada** com a indicador per tal d'obtenir alertes més robustes i fiables.

Respecte a això, el document destaca com l'ús de valors mitjans d'una única dada per definir una alerta augmenta el risc de generar falsos positius. Per tal d'evitar aquest risc, una possible estratègia és precisament definir l'alerta combinant diverses dades, relatives a diferents aspectes del fenomen analitzat, per tal de generar un indicador compost més fiable.

Tercera idea: la importància crucial de la **disponibilitat i qualitat de les dades** a utilitzar. El disseny d'alertes requereix necessàriament disposar de dades en quantitat suficient —per permetre la comparació i l'establiment de valors mitjans de referència, que permetin detectar anomalies— i de qualitat —les dades han de ser fiables i no han de contenir errors ni mancances significatives—.

El document destaca especialment l'interès de creuar i analitzar conjuntament les dades de contractació pública, en sentit estricte, i dades d'altres tipus —tot i que, evidentment, relacionades amb la contractació— com serien dades mercantils, financeres, de titularitats reals d'empreses, de vinculacions entre entitats, etc.

Tornarem sobre aquesta important qüestió en tractar la tipologia de sistemes d'alerta en l'apartat 4.3 següent.

3.3.3 Metodologia

L'apartat III del document *Red Flags for Integrity* resulta especialment interessant als efectes del present estudi en la mesura en que presenta els **5 passos metodològics** seguits per a la creació del llistat de possibles alertes del document complementari [67].

d. el frau, referit a la fase d'execució dels contractes, una vegada adjudicats, que inclouria també vàries tipologies d'irregularitats —incompliments contractuals, falsa facturació, modificacions irregulars, etc.—.

[67] *Op. cit.* pàg. 12: «La nostra aproximació a la detecció de la corrupció és simple: hem compilat alertes de risc de corrupció al llarg del cicle de contractació, desenvolupat indicadors per cada alerta i definit aquestes alertes mitjançant còmputs clars i replicables. Hem definit llavors aquests còmputs utilitzant els camps de dades de l'estàndard OCDS, permetent que qualsevol que disposi d'aquest estàndard pugui calcular els indicadors. El passos següents inclouen posar a prova els

L'interès d'aquest passos metodològics és d'allò més gran que són **generalitzables i extrapolables a qualsevol procés de disseny i implantació d'un sistema d'alerta** en qualsevol organització. Per això, a continuació i al fil de l'exposició d'aquells passos, anirem apuntant en quins termes es podrien adaptar, al nostre entendre, al procés concret de disseny i implantació d'un sistema d'alerta.

Els cinc passos metodològics són els següents:

Primer: **identificar les possibles alertes**. El primer pas dels autors del document que ens ocupa va ser recopilar un llistat d'alertes, de possibles indicadors de riscos d'irregularitats, frau o corrupció en els processos de contractació pública. La perspectiva generalista del document, i la seva vocació de referent en l'àmbit que ens ocupa determina que la recopilació que van fer fos el més àmplia i omnicomprensiva possible, intentant establir qualsevol alerta que es considerés «observable, col·leccionable i rellevant».

Ara bé, en qualsevol organització que aspiri a dissenyar i implementar un sistema automatitzat d'alerta aquest primer pas és igualment important, no tant amb l'objectiu de llistar *totes* les possibles alertes imaginables —per això ja existeix el document complementari d'OCP amb el llistat de 73 possibles alertes—, sinó per establir **quines alertes concretes són útils i rellevants ateses les característiques de l'organització**.

Efectivament, sembla evident que el sistema d'alerta adient per a un ajuntament petit o mitjà amb limitacions i deficiències de capacitat de gestió administrativa no serà el mateix per a un gran ens local amb una estructura organitzativa àmplia i de gran capacitat o per a una entitat gestora de grans infraestructures: es pot raonablement conjecturar que les alertes més rellevants i útils en el primer cas es centraran en aspectes procedimentals —fraccionaments derivats de deficiències de planificació i gestió; situacions irregulars de continuïtat de prestacions de contactes ja conclosos, per exemple—; en el segon probablement tindran importància la detecció de situacions de conflicte d'interès o irregularitats en la fase d'execució; i en el tercer serà molt més útil posar el focus en possibles riscos de col·lusió...

Com ja hem vist, i remarca el document que comentem, el context és rellevant.

Segon: **definir cada alerta**. Es tracta ara de «transformar cada alerta en un indicador discret i quantificable», el que requereix determinar exactament quina o quines dades concretes caldrà utilitzar per definir l'alerta, quines són les relacions lògiques entre les diverses dades —quan s'utilitzi més d'una dada— i quin o quins són els valors llindars de la dada o de cadascuna de les dades que desencadenen l'alerta.

En aquest pas es definirà igualment la naturalesa i, en el seu cas, els valors possibles de l'alerta. Així, una alerta de caràcter binari només podrà tenir dos

indicadors utilitzant diverses fonts de dades OCDS per avaluar la seva integritat en els diversos mercats de contractació pública».

valors: positiu o negatiu —es dona la situació irregular que l'alerta detecta o no es dona—; en canvi, un indicador de risc en sentit estricte podrà donar un gradient de valors —per exemple valors entre 0, corresponent a la inexistència de risc, i 10, corresponent al màxim risc—.

Tercer: **assignar a cada alerta un tipus o esquema d'irregularitat, frau o corrupció específic**. Aquest pas, molt lligat a l'anterior, implica establir clarament quin és el significat de l'alerta.

Recordem que una alerta no significa necessàriament una prova plena i categòrica de l'existència d'una —o vàries— irregularitat o supòsit de frau o corrupció; una alerta sovint indica que es dona una circumstància que justifica una revisió o investigació més acurada. Això implica tenir clarament establert què significa l'alerta, el que determinarà què és el que s'ha de revisar i/o investigar.

Per exemple, una alerta que indiqui l'existència d'un licitador únic, en el cas d'una licitació on raonablement s'espera un nivell de competència elevat —atès el mercat i/o els precedents— pot significar diverses coses: una errònia fixació del tipus de licitació, uns criteris de selecció qualitativa dels licitadors massa restrictius, la publicació de l'anunci de licitació en un moment inadequat —per exemple a principis o mitjans del mes d'agost—, una alteració conjuntural o no de l'estructura del mercat, però també l'existència de col·lusió entre els potencials licitadors. Per tant, en la subsegüent revisió caldrà analitzar tant el disseny de la licitació —plecs de clàusules— i la tramitació del procediment com les característiques i actuals del mercat, etc.

D'altra banda, tal i com encertadament destaca el document que comentem, no és inusual que saltin diverses alertes respecte d'una mateixa licitació o d'un mateix contracte; evidentment, en aquests casos les probabilitats que efectivament s'hagi produït o s'estigui produint algun tipus d'irregularitat, frau o corrupció són més elevades.

Quart: **mapejar les dades de l'alerta d'acord amb l'estàndard OCDS**. Del que es tracta, en aquest pas, és de subsumir les dades concretes utilitzades en cada alerta en el model de dades OCDS. Evidentment aquest pas metodològic era ineludible pels autors del document *Red Flags for Integrity*, atesa la seva pretensió d'establir un llistat el més ampli i omnicomprensiu d'alertes com és el del document complementari, i de definir les alertes d'acord amb un model de dades i una terminologia generalment comprensible i fàcilment aplicable per a qualsevol organització interessada —el que, òbviament, portava a la utilització de l'estàndard OCDS, creat per OCP—. És igualment evident que aquest pas no és estrictament necessari en qualsevol organització que pretengui dissenyar i implantar un sistema d'alerta.

No obstant, l'ús de l'estàndard de dades obertes de contractació pública OCDS es pot considerar una bona pràctica que presenta interessants beneficis: major facilitat a l'hora d'implementar les alertes que interessin de les 73 del llistat del document complementari d'OCP; utilitat en la implementació d'una política de dades obertes de contractació; comparabilitat de les dades pròpies amb les

d'altres organitzacions nacionals o internacionals i, per tant, comprovació de la validesa de les alertes dissenyades amb dades d'altres orígens.

Cinquè: **assignar cada alerta a la corresponent fase del cicle de contractació**. En general se solen distingir cinc fases en el cicle o procés complet de contractació: la preparació o planificació, la licitació, l'adjudicació, la formalització i l'execució del contracte. És doncs convenient determinar, per a cadascuna de les alertes concretes identificades i definides, a quina d'aquelles fases del cicle de contractació es refereix. Això permet tenir una visió clara de si **el sistema d'alerta establert cobreix de forma homogènia i consistent tot el cicle** de contractació, o si només es focalitza en alguna o algunes de les fases del mateix.

Respecte a això, és molt significativa una observació dels autors del document *Red Flags for Integrity*: tot i l'amplíssima recopilació de possibles alertes que van dur a terme, constaten que «moltes més alertes es poden calcular en les fases de licitació i adjudicació que en les de formalització, execució i planificació» i, per tant, apunten com a possibilitat d'evolució i de millora del document, entre d'altres, la incorporació de noves alertes centrades en la fase de planificació on «la teoria ens diu que existeixen nombroses oportunitats per a actuacions il·lícites» [68].

En aquest mateix sentit, és interessant portar a col·lació la següent observació del capítol I del bloc VII de la *Guía de integridad en la contratación pública local*, publicada per la FEMP al març de 2019 [69]:

> *«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 —*

[68] *Op. cit.* pàg. 27.

[69] Accessible a: http://femp.femp.es/files/3580-2053-fichero/GUIA_INTEGRIDAD_CONTRATACION_PUBLICA_LOCAL.pdf.

mientras haya crédito suficiente en la partida correspondiente—, estamos al cabo de la calle.

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.»

Aquest advertiment i posada en guàrdia és perfectament aplicable en l'àmbit que ens ocupa, a l'hora de dissenyar un sistema d'alerta: tot el cicle de la contractació pública ha d'estar cobert per les alertes que s'implementin, i la fase d'execució dels contractes de cap manera pot considerar-se secundària o menys important, sent especialment crítica i important la identificació i recopilació de les dades d'aquesta fase.

Per concloure aquesta breu referència al document *Red Flags for Integrity*, quatre breus apunts addicionals:

a. el document insisteix reiteradament en la conveniència i utilitat d'adoptar l'estàndard OCDS que va molt més enllà de l'establiment de sistemes d'alerta;

b. el document, amb un encomiable afany pedagògic, conté sis exemples de definició d'alertes concretes[70], per a cadascuna de les quals es defineix i s'explica l'alerta, es detallen les dades del model OCDS utilitzades per calcular-la, s'inclou l'algoritme en llenguatge R —un dels llenguatges de programació d'algoritmes per a l'anàlisi i explotació de dades més usuals— per al seu càlcul i s'inclou igualment una explicació literal del codi en llenguatge R;

c. el document conté igualment una detallada explicació del contingut del document complementari *Red Flags to OCDS Mapping*, en format de full de càlcul, així com una anàlisi de les dades del model OCDS amb major utilitat als efectes d'alertes —dades amb major nombre d'utilització en diferents alertes; dades amb utilitat com a alertes per si soles—; i

d. finalment, el document tracta de recapitular les principals lliçons que es poden extreure de la tasca realitzada, identificar les mancances existents i possibilitats d'evolució i millora, i analitza el funcionament dels sistemes d'alerta realment existents basats en l'OCDS, especialment el d'Ucraïna.

[70] Els sis exemples d'alertes tractats són els següents:

a. licitador únic: alerta indicativa de la inexistència de concurrència efectiva en la licitació;

b. termini excessivament curt de presentació d'ofertes: alerta indicativa de possible favoritisme per part de l'entitat contractant en benefici d'un licitador que disposaria d'informació sobre la licitació abans de la seva publicació;

c. licitador novell en una licitació: alerta indicativa d'una alteració en el mercat concernit;

d. baixes mínimes en una licitació: alerta indicativa de possible col·lusió entre licitadors o d'una errònia o irregular fixació del tipus de licitació;

e. baixes amb intervals regulars entre elles: alerta indicativa de possible col·lusió; i

f. exclusió de tots els licitador excepte l'adjudicatari: alerta indicativa de possibles irregularitats en l'establiment dels criteris de selecció qualitativa dels licitadors.

En definitiva, ens trobem davant d'un document, alhora teòric i pràctic, sistemàtic i metodològic, enormement pedagògic que constitueix una de les millors recapitulacions i síntesis de la matèria que ens ocupa.

4 Anàlisi

Hem identificat el context en el qual s'ha de situar el present estudi; hem repassat l'estat de situació existent; i ens hem detingut en tres referents indefugibles com són l'eina Arachne, el sistema SALER i el document *Red Flags for Integrity* d'OCP.

Arribats a aquest punt, estem en condicions de desenvolupar algunes reflexions i consideracions que considerem rellevants.

4.1 Prevenció i contingència

Tal i com encertadament destaquen Roger FOLGUERA FONDEVILLA i Lara BAENA GARCÍA al seu article monogràfic ja citat[71], una bona gestió integral dels riscos d'irregularitats, de frau o de corrupció ha d'incloure dues perspectives o dimensions: la preventiva i la contingent.

L'**actuació preventiva** té per objectiu reduir la probabilitat que els riscos per a la integritat en una institució es produeixin efectivament, es materialitzin, mentre que l'**actuació contingent**, pel contrari, se centra en reduir l'abast i la gravetat dels danys i perjudicis produïts quan els riscos s'han arribat a materialitzar.

Doncs bé, sobre això el document *Red Flags for Integrity* apunta una idea disruptiva en l'àmbit que considerem: **la capacitat dels sistemes d'alerta basats en l'anàlisi de dades de fer convergir ambdós paradigmes, el preventiu i el contingent**.

Hem vist com els sistemes d'alerta permeten detectar les possibles irregularitats i els riscos potencials de frau i corrupció abans que s'arribin a materialitzar; en aquest sentit, el document *Red Flags for Integrity* insisteix en el caràcter intrínsecament proactiu d'aquests sistemes d'alerta[72].

Cal però matissar aquesta afirmació: l'element clau aquí és la capacitat d'explotar les dades de contractació pública ***en temps real***.

Efectivament, cal distingir entre sistemes d'alerta basats en l'anàlisi de dades que funcionen en temps real, analitzant les dades i, en el seu cas, generant les alertes corresponents a mesura que es generen les dades, en cada tràmit i fase del corresponent procediment de contractació, i sistemes d'alerta basats en dades que funcionen *a posteriori*, analitzant les dades i generant les alertes amb posterioritat —més o menys lluny en el temps— a la realització dels esdeveniments que, datificats, generen les dades utilitzades.

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

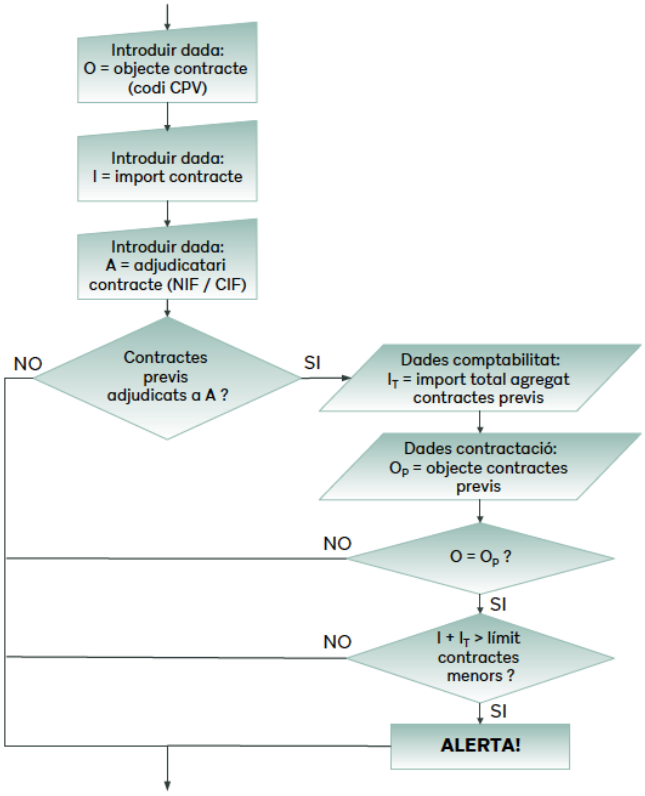
[72] Cfr. apartat 3.3.1 anterior (pàg. 50 i 51) i notes 63 i 64.

En el primer cas, prevenció i contingència convergeixen: el fet que l'alerta permeti detectar la irregularitat en el moment en el qual es produeix **permet igualment evitar-la** i, per tant, **reduir a zero els danys o perjudicis causats**. En el segon cas, òbviament, les alertes que permeten la detecció d'irregularitats, frau o corrupció *a posteriori* són, paradigmàticament, instruments d'actuació contingent.

Il·lustrem aquesta idea amb un exemple: el fraccionament de contractes per tal d'eludir els procediments de contractació amb publicitat i concurrència.

Un sistema d'alerta pot obtenir, de fonts internes o de fonts obertes —dades obertes de contractació— la relació de contractes menors i/o de contractes adjudicats sense cap procediments amb publicitat i concurrència i, analitzant aquestes dades, detectar els casos en els quals s'han produït diverses adjudicacions al mateix contractista de contractes amb objecte idèntic o semblant, en un curt període de temps —posem un any—, de manera que l'import total agregat d'aquelles diverses adjudicacions a un mateix contractista superi significativament els límits de la contractació menor. Això hauria de desencadenar una alerta de fraccionament: existeixen indicis —no necessàriament proves concloents; aquestes s'haurien d'obtenir mitjançant la revisió o investigació que l'alerta hauria de desencadenar— que s'ha fraccionat la prestació que es tracti en diversos contractes per poder adjudicar-los tots, eludint els requisits normatius de publicitat i concurrència, a un mateix contractista. Estem davant d'un mecanisme contingent: el risc —que es produeixi fraccionament— ja s'ha materialitzat, i, si es verifica que efectivament s'ha produït fraccionament il·legal, és a dir, que no existeixen raons excepcionals, legalment admeses i previstes, que justifiquin aquella situació, l'únic que es podrà fer és dur a terme actuacions per revertir les situacions il·legals produïdes —la revisió d'ofici de les adjudicacions dels contractes, per ex.—, minimitzar els danys produïts —suspendre en el seu cas els contractes no totalment executats; imposar sancions o penalitzacions— i, com a mínim, evitar la seva perpetuació o reproducció en el futur —reforçar els mitjans de control intern; depurar responsabilitats—.

Ara bé, podem igualment concebre un sistema d'alerta, necessàriament basat en dades internes —si hem d'esperar a la publicació de les dades, serà massa tard i ens trobarem en l'escenari anterior—, que detecti, en el moment en que es vagi a produir l'adjudicació d'un contracte, l'acumulació de contractes amb el mateix objecte —o un objecte *a priori* coincident: mateix codi CPV— en el mateix contractista per un import agregat que superi els límits de la contractació menor. El mecanisme, descrit en termes d'un diagrama de flux, es podria representar, simplificadament, de la manera següent:



Amb un sistema com aquest [73], és possible, en els casos en què es produeixi l'alerta, adoptar mesures per evitar que el risc de fraccionament s'arribi a materialitzar.

Quines mesures? Aquí les opcions són diverses, i depenen de criteris i decisions de gestió que no es poden fixar de manera categòrica i general, atès que dependran en gran mesura de les possibilitats i característiques organitzatives de cada entitat. Vegem-ne algunes:

a. una primera opció, molt radical, és que quan salti l'alerta el sistema simplement no permeti l'adjudicació del contracte a l'adjudicatari inicialment previst: senzillament el sistema —el gestor electrònic d'expedients de contractació— no ho permet i, per tant, el servei gestor de l'expedient haurà de buscar un altre contractista a qui adjudicar aquell contracte —o desistir de la contractació, és clar—;

b. però també és possible que en aquests casos el sistema exigeixi al servei gestor un informe addicional justificant les raons i els fonaments legals que justificarien l'adjudicació del contracte al contractista inicialment previst —p. ex. la inexistència de competència respecte de la prestació objecte del contracte per raons tècniques o de protecció de drets exclusius, *ex* art. 168 a) 2n de la LCSP—;

c. també és possible que el sistema permeti l'adjudicació i que l'alerta doni lloc a una revisió o auditoria, pels òrgans de control interns de l'ens de que es tracti, de tots els expedients de contractació adjudicats a la mateixa

[73] Segons la informació de que disposem l'Ajuntament de Santa Coloma de Gramenet disposa d'un sistema molt semblant al que es descriu en aquest exemple.

empresa; en aquest cas, el mecanisme d'alerta tindria un caràcter més contingent que efectivament preventiu.

Les possibilitats són nombroses i és difícil establir apriorísticament i amb caràcter general una única opció com a correcta. En aquest sentit, l'opció radical abans apuntada —el sistema impedeix categòricament i sense alternatives l'adjudicació del nou contracte a l'adjudicatari previst— pot generar situacions de bloqueig i disfuncions en administracions amb dèficits de capacitat de gestió que donin lloc a problemes més greus que els que es pretenen evitar.

No obstant, el fet és que els sistemes d'alerta obren possibilitats reals d'incidir en temps real sobre els riscos potencials i, en aquest sentit, fan convergir i aproximar-se, com hem dit, els dos grans paradigmes, prevenció i contingència, de la gestió dels riscos d'irregularitats, frau i corrupció.

4.2 Sistemes externs vs. interns

L'exemple de l'apartat anterior ens porta a una segona reflexió, centrada en la distinció entre sistemes d'alerta que designarem com *interns* i *externs*, d'acord amb les definicions següents:

a. designarem com a **sistemes externs** els sistemes d'alerta que funcionen amb dades obtingudes de fonts diferents al propi gestor electrònic d'expedients de contractació i que, per tant, no tenen *a priori* capacitat per interactuar en temps real, directament i automatitzada, amb aquest —o, si la tenen, és més o menys limitada—; i

b. designarem com a **sistemes interns** els sistemes que obtenen les dades directament del gestor electrònic d'expedients de contractació i poden interactuar amb aquest en temps real.

Aquesta distinció és rellevant en la mesura en que molts —probablement la majoria— dels projectes i estudis sobre sistemes d'alerta es basen en dades obertes[74] i, per tant, es configuren més com a sistemes contingents que com a sistemes realment preventius.

Efectivament, el fet que un sistema d'alerta es nodreixi de dades obertes, tant si les dades s'obtenen ja estructurades i directament explotables d'un portal de transparència o de dades obertes o del RPC, com si s'obtenen mitjançant tècniques de *scraping*[75] i, eventualment, són posteriorment objecte d'estructuració i depuració per al seu ulterior tractament, introdueix

[74] Aquest és el cas, entre molts altres, del projecte DIGIWHIST del projecte hongarès Red Flags, ja esmentats. Cfr. apartat 1.3 anterior (pàg. 8) i notes 2 i 3.

[75] El ***scraping*** és la tècnica consistent en l'extracció automatitzada, mitjançant una aplicació *ad hoc*, de dades accessibles i llegibles, normalment en una pàgina web; dit en d'altres paraules, es tracta d'extreure automatitzadament les dades d'una determinada font, el que dona com a resultat una base de dades, p. ex. un arxiu en format Excel. El fet que la base de dades s'obtingui a través d'aquell procés fa que sovint les dades així obtingudes presentin errors o mancances, el que determina que sigui necessari, abans de la seva explotació, procedir a la seva neteja —eliminació de redundàncies, correcció d'errors, estructuració i homogeneïtzació, etc.—, i, en general, siguin de menor qualitat.

inevitablement un retard que impossibilita que l'alerta incideixi en temps real en la tramitació del procediment de contractació i, per tant, limita l'eficàcia del sistema a la vessant contingent: el sistema permetrà detectar irregularitats una vegada ja s'hagin produït, però només indirectament i amb caràcter prospectiu permetrà evitar que es produeixin; el que ha passat ha passat —les irregularitats detectades a partir de l'anàlisi de les dades— i ja només es podrà plantejar evitar que es perpetuï o es reprodueixi mitjançant l'adopció o implementació *a posteriori* de mesures correctores.

Respecte a això cal tenir present, si considerem un sistema d'alerta basat que obtingui les dades del RPC, que el termini per a la tramesa de les dades al Registre és d'un mes des de la data de formalització del contracte o des de la data de l'aprovació de la modificació, pròrroga, incidència, conclusió o liquidació[76]. La impossibilitat d'una reacció en temps real és doncs evident. I si considerem un hipotètic sistema d'alerta basat en dades obtingudes mitjançant *scraping* de la PSCP, probablement podrem escurçar el temps de reacció però és igualment evident que subsisteix en gran mesura la impossibilitat d'incidir en temps real en la tramitació del procediment —sense comptar els problemes afegits derivats del procés mateix d'obtenció de les dades per aquella via—.

La **superioritat dels sistemes interns** és doncs, des d'aquest punt de vista, indiscutible. I, per tant, seria desitjable centrar els esforços en el desenvolupament de sistemes d'alerta de caràcter intern que es nodreixin de dades directament obtingudes dels gestors electrònics d'expedients —el que evidentment només serà possible si es disposa d'un gestor integrat que cobreix tot el procediment de contractació; si una part del procediment no està automatitzada ni, per tant, datificada, la limitació estructural és evident— i es dissenyin amb capacitat per interactuar automatitzadament amb el gestor d'expedients, per garantir l'efecte realment preventiu de les alertes.

D'aquesta idea podem derivar dos corol·laris, un de molt concret i un altre de molt més general.

Concretament, si tornem de nou la iniciativa del Consorci Localret per a dotar els ens locals d'una eina de seguiment, control i planificació de la contractació, ja comentada[77], recordem com l'informe sobre els resultats de la consulta de mercat duta a terme recollia, pel que fa específicament a l'obtenció de dades, la distinció que ara considerem, entre solucions integrades de contractació electrònica, que obtenen les dades «directament del tramitador d'expedients o de l'eina de licitació electrònica» —solucions internes—, i solucions específiques no incloses en una eina de contractació electrònica, que «obtenen les dades (dels contractes) des de les plataformes públiques de contractació: PLACE i/o PSCP [...] o també del Registre Públic de Contractes (RPC)» —solucions externes—.

[76] Així ho disposa l'art. 3 de l'Ordre ECO/47/2013, de 15 de març, per la qual es regula el funcionament i s'aprova l'aplicació del Registre públic de contractes de la Generalitat de Catalunya.

[77] Cfr. apartat 2.3.3 anterior (pàg. 35).

Doncs bé, en la mesura que sigui possible seria desitjable que s'apostés i s'afavorís tot el possible les primeres d'aquelles solucions, de caràcter intern, especialment de cara a la implementació en aquella solució d'un sistema automatitzat d'alerta.

I si considerem ara la disjuntiva que ens ocupa des d'un perspectiva molt més general, no podem deixar d'apuntar un risc inherent a la idea mateixa dels sistemes externs d'alerta, que és el següent.

Ja hem assenyalat com la idea d'utilitzar les dades obertes de contractació com a instrument de lluita contra la corrupció és un paradigma globalment consolidat [78]. I acabem de veure com molts dels projectes de sistemes d'alerta responen a aquest paradigma basant-se precisament en dades obertes o en dades obtingudes de les plataformes de contractació electrònica.

Doncs bé, sense qüestionar en absolut —ans al contrari— l'afirmació de que «les dades obertes contribueixen a la prevenció, la detecció, la investigació i la reducció de la corrupció» [78], en els treballs d'elaboració del present estudi hem pogut detectar el risc difús d'**una invocació desviada d'aquell principi** que es concretaria en la idea de prioritzar i centrar tots els esforços en la transparència i la implementació de dades obertes assumint implícitament que això, en la mesura que possibilita i afavoreix el desenvolupament de sistemes d'alerta de caràcter extern, dona satisfacció a l'objectiu de desenvolupar sistemes d'alerta basats en dades.

I evidentment no és així.

Els sistemes d'alerta basats en dades no han de concebre's com una finalitat en si mateixa, sinó com **un instrument de control al servei de la integritat**. I el primer i principal nivell de control, en tota organització i especialment en el sector públic és el **control intern**. Defugir les responsabilitats i l'enfortiment del control intern perquè existeix o pot existir un control extern és absurd i pervers: és evident que **on cal implementar els mecanismes i els instruments més eficients de detecció d'irregularitats i de potencials fraus i corrupcions és en l'àmbit intern**, com a eines al servei de les instàncies de control intern, especialment quan aquestes instàncies disposen de recursos i mitjans limitats o insuficients, com és sovint el cas en l'àmbit local.

4.3 Tipologia: 3 nivells de sistemes d'alerta

Hem vist com el document *Red Flags for Integrity* d'OCP destacava especialment l'interès d'analitzar conjuntament, creuant-les, tant les dades de contractació pública, en sentit estricte, com dades d'altres tipus —tot i que òbviament relacionades amb la contractació— com serien dades mercantils, financeres, de titularitats reals d'empreses, de vinculacions entre entitats, etc.

[78] *Principis de dades obertes anticorrupció*, aprovats pel G20 al 2015, ja citats. Cfr. apartat 2.1.2 anterior i nota 16 (pàg. 17).

Aquesta important idea ens permet establir una **tipologia dels sistemes d'alerta**, distingint **3 nivells** que, en ordre creixent de capacitat de detecció d'irregularitats, fraus i corrupció, serien els següents:

4.3.1 Nivell 0: el gestor electrònic d'expedients

Tot gestor electrònic d'expedients de contractació, adequadament dissenyat i configurat, pot **fer la funció i servir com a sistema automatitzat d'alerta** i prevenir que es materialitzin alguns tipus d'irregularitats. Efectivament, si pressuposem un disseny correcte i una configuració conforme amb els requisits i imperatius legals, el gestor d'expedients estructura i articula la tramitació del procediment d'acord amb el marc legal, impedint o bloquejant la tramitació —o, com a mínim, generant una alerta—si en algun punt no es compleixen els requisits legals o no es respecten els tràmits.

Així, per exemple, si no es carrega en el gestor l'informe o l'acord motivant la necessitat del contracte que preveu l'art. 116.1 de la LCSP, amb el contingut estipulat a l'apartat .4 d'aquell precepte, o si no es carreguen els documents exigits pel seu apartat .3, el gestor no hauria de permetre passar al tràmit següent, d'aprovació de l'expedient —art. 117.1 de la LCSP—.

Ara bé, el gestor electrònic d'expedients de contractació, com a sistema d'alerta, presenta però **limitacions molt importants** en la mesura que pot garantir el compliment *purament formal* del procediment però no el compliment substancial del marc legal —p. ex. difícilment detectarà que un informe preceptiu contingui errors grollers o estigui buit de contingut—.

D'altra banda, l'eficàcia i la utilitat de determinades alertes, implementades a aquest nivell bàsic, en el gestor electrònic d'expedients de contractació, és molt relativa —i fins i tot pot arribar a ser nul·la—. Efectivament, determinades circumstàncies que constitueixen indicadors objectius de risc poden ser, aïlladament considerades, plenament compatibles amb el marc legal i, per tant, *a priori*, hi haurien d'aturar la tramitació en curs i, si donen lloc a una alerta, probablement se l'hagi de descartar com a fals positiu.

En aquest sentit i a títol d'exemple, el fet que en una licitació per procediment obert, amb tota la publicitat legalment exigible i un termini suficient de presentació d'ofertes, es presenti única oferta pot ser indicatiu de diversos riscos: una licitació a mida o un acord col·lusori entre potencials licitadors; però si l'oferta és conforme amb les exigències del plec de clàusules i racional i raonable, *a priori* el contracte s'hauria d'adjudicar.

I, sobretot, la principal limitació del gestor d'expedients com a sistema d'alerta és que només pot tenir en compte les dades del procediment concret que s'hi està tramitant, el que impedeix detectar irregularitats que s'articulen mitjançant un conjunt de procediments, legals aïlladament considerats però irregulars —o fins i tot delictius— considerats en conjunt: paradigmàticament, aquest seria el cas del fraccionament il·legal de contractes.

Aquesta consideració ens porta al següent nivell d'un sistema d'alerta.

4.3.2 Nivell 1: explotació de les dades de contractació i comptabilitat

Per superar aquelles limitacions, és necessari que el sistema d'alerta tingui accés i exploti no només les **dades del procediment concret que s'està tramitant** sinó igualment, i de forma simultània, les **dades de tota la contractació pública** de l'ens que es tracti així com les **dades comptables corresponents** —que, de fet, són la vessant quantitativa, el reflex econòmic de la contractació—.

En aquest nivell el sistema d'alerta **articula la interacció entre el gestor d'expedients i les bases de dades de contractació i comptabilitat** que contenen informació, que va més enllà del concret procediment que es tramita.

L'exemple que hem presentat anteriorment[79] d'una possible alerta que detecti el fraccionament de contractes per tal d'eludir els procediments de contractació amb publicitat i concurrència il·lustra perfectament aquesta idea. En el diagrama de flux que descriu el funcionament d'aquella alerta es veu clarament com les dades del contracte concret que s'està tramitant —import, I, i objecte, O— es comparen amb les dades extretes de la comptabilitat —import total agregat, I_T, dels contractes adjudicats al contractista al qual es pretén adjudicar el contracte que s'està tramitant— i de la contractació anterior de l'ens considerat —objecte, O_P, dels contractes prèviament adjudicats a l'esmentat contractista—.

És important indicar que el GEEC, que com hem vist[80] té prevista normativament la seva integració amb els sistemes econòmics i financers corporatius de la Generalitat de Catalunya (GECAT i Pangea), l'RPC, la PSCP i d'altres bases de dades, plataformes i sistemes, suportaria per tant sense requerir adaptacions substancials un sistema d'alerta d'aquest nivell.

Quant a l'eina de seguiment, control i planificació pels ens locals objecte de la iniciativa del Consorci Localret[81] hem vist igualment com es preveu l'obtenció de dades directament dels gestors d'expedients en cas de solucions integrades de contractació electrònica o de les plataformes públiques de contractació i de l'RPC en el cas de solucions no integrades —òbviament, com ja hem indicat en l'apartat 4.2 anterior, menys interessants—. Tractant-se d'una iniciativa encara en curs de desenvolupament seria especialment interessant afavorir les solucions que no només incorporin l'accés a les dades de contractació sinó igualment a les de comptabilitat.

Ara bé, una ràpida ullada a les alertes detallades en el llistat complementari al document *Red Flags for Integrity* permet constatar que el creuament de les dades d'un concret procediment en tramitació amb les dades de contractació i de comptabilitat de l'entitat contractant, tot i que permet detectar nombroses alertes, presenta igualment limitacions: moltes altres alertes requereixen altres

[79] Cfr. apartat 4.1 anterior (pàg. 59 i seg.).

[80] Cfr. apartat 2.3.1 anterior (pàg. 27).

[81] Cfr. apartat 2.3.3 anterior (pàg. 35).

dades que, *a priori*, no consten en aquelles dues bases de dades, com, exemple de nou paradigmàtic, les vinculacions entre empreses licitadores.

Això ens porta al següent nivell dels sistemes d'alerta.

4.3.2 Nivell 2: creuament amb d'altres dades internes i externes

El model dels sistemes d'alerta d'aquest nivell són els dos referents que hem estudiat: l'eina Arachne de la Comissió Europea i el sistema SALER de la Comunitat Valenciana.

En aquest nivell, el sistema d'alerta es nodreix i explota **dades de tres fonts**:

a. les dades del gestor electrònic d'expedients de contractació, referides al procediment concret que s'està tramitant;

b. les dades de contractació i de comptabilitat de l'entitat considerada, de caràcter intern —això, en tot cas, és desitjable, tot i que eventualment, a falta d'una millor opció, es pugui plantejar, com hem vist, l'obtenció de les dades de contractació de fonts externes: PSCP, RPC o altres—; i

c. dades addicionals de caràcter extern: dades mercantils —del Registre Mercantil—, de solvència —RELI, per ex.—, de nomenaments en càrrecs públics o privats, dades econòmiques i financeres —bases de dades d'informació econòmica de societats—, i fins i tot —tal i com hem vist que preveu la regulació del sistema SALER— dades obertes d'Internet.

Evidentment, aquest és el nivell idoni i, per tant, el disseny i projecte d'implementació de qualsevol sistema d'alerta hauria d'aspirar a situar-s'hi. No obstant, no podem obviar algunes problemàtiques rellevants que es plantegen a aquest nivell.

La primera fa referència a la **complexitat del sistema**. En aquest nivell, des d'un punt de vista tècnic, el sistema d'alerta excedeix clarament el que és un gestor electrònic d'expedients de contractació, pròpiament dit. El sistema d'alerta difícilment es pot plantejar com a part del gestor d'expedients, sinó que més aviat s'ha de concebre com un sistema autònom. En efecte, la interacció d'un gestor d'expedients amb les dades de contractació i de comptabilitat, i la seva integració amb els sistemes de gestió financera, econòmica i comptable és quelcom que ja existeix —el GEEC de la Generalitat de Catalunya n'és un exemple, però existeixen igualment moltes altres solucions integrades que ofereixen aquesta possibilitat—; i, per tant, la implementació de sistemes de nivell 1 no planteja, *a priori*, grans problemes tècnics.

Ara bé, quan considerem sistemes de nivell 2, que han d'interaccionar amb bases de dades externes i eventualment explotar dades obertes la situació és diferent: estem parlant de sistemes d'alerta que, òbviament, interactuen amb el gestor d'expedients però que constitueixen tècnicament un sistema diferent. Tot i que aquest tipus de sistemes són, al nostre entendre, l'objectiu a assolir, els reptes tècnics a aquest nivell són certament molt més importants.

En aquell nivell el principal repte se situa en el nivell de **compromís de les institucions amb la integritat**. En el context en el qual ens trobem, qualsevol impuls a la digitalització de les administracions públiques hauria d'incorporar la integritat com a principi nuclear essencial. Tots els desenvolupaments digitals per al sector públic haurien d'incorporar el **principi d'*integritat per disseny*** en la seva concepció i implementació i, per tant, incorporar mecanismes de detecció i prevenció de riscos per a la integritat no com una opció complementària sinó un element integrant de l'estructura principal vertebradora de tota solució tecnològica per a l'àmbit de la contractació pública. Aquell principi general hauria de ser inspirador i director de qualsevol actuació o desenvolupament en aquest àmbit.

La segona problemàtica que es planteja a aquest nivell es refereix a la cobertura jurídica, des del punt de vista del marc legal de **protecció de dades personals**, de l'**ús de les dades en els sistemes d'alerta** d'aquest nivell. Efectivament, una de les alertes més importants i transversals a tot el cicle de la contractació pública —en la mesura que correspon a un risc que es pot donar en cadascuna de les fases de la contractació: preparació o planificació, licitació, adjudicació, formalització i execució del contracte— és la de detecció de possibles conflictes d'interès i, evidentment, la implementació d'aquesta alerta necessàriament comporta l'explotació i el tractament de dades personals.

Analitzada la qüestió des d'aquesta perspectiva, no sembla que l'ús de les dades personals del propi procediment de contractació plantegi cap problema, atesa la previsió de l'art. 6 c) del RGPD i la seva transposició en l'art. 8.1 de la LO 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD), que habilita al tractament de les dades per al compliment d'una obligació legal, posada en relació amb l'imperatiu de prevenció dels conflictes d'interessos de l'art. 64 de la LCSP. Tampoc sembla que plantejaria problemes l'ús de dades personals que constin en registres públics amb finalitat de publicitat i propòsit general, com seria el cas del Registre Mercantil. L'ús de dades personals d'altres expedients de contractació —extretes pel sistema d'alerta de la corresponent base de dades— igualment es podria entendre —tot i que no de manera tan evident— emparada per les referides previsions legals. Però sembla clar que l'ús de dades obertes obtingudes d'Internet requeriria una habilitació legal específica, d'acord amb el que preveu l'art. 8.3 de la LOPDGDD.

En aquest sentit, seria desitjable poder **comptar amb una previsió normativa expressa de rang legal** —idealment en la LCSP o eventualment en la normativa catalana de desenvolupament de la mateixa—, de la mateixa manera que el sistema SALER es troba emparat per les previsions de l'art. 17.3 de la Llei 22/2018 [82].

La tercera problemàtica —i potser la més important— fa referència als **recursos que fa necessària l'existència mateixa d'un sistema d'alerta**, especialment si és un sistema del màxim nivell i, per tant, té una gran capacitat de detecció de diversos tipus de possibles irregularitats.

[82] Cfr. apartat 3.2 anterior (pàg. 48 i 49).

Efectivament, a mesura que s'incrementa el nivell d'un sistema d'alerta i creix, per tant, la seva capacitat de detecció d'irregularitats, fraus i corrupció, esdevé més i més crític disposar de recursos per gestionar les alertes generades. Si considerem alertes que no comporten un bloqueig automàtic de la tramitació de l'expedient i que no indiquen inequívocament l'existència d'una irregularitat, sinó una alta probabilitat —però no la certesa— de materialització d'un risc, és evident que implementar un sistema d'alerta sense dotar a l'òrgan responsable de la gestió i explotació del sistema d'uns mínims recursos no té cap sentit. Les alertes tenen utilitat si permeten reaccionar en temps real. Però si la falta de mitjans impedeix qualsevol mena de reacció, o només permet reaccions *a posteriori* en forma de constatació dels perjudicis causats, ja irreversibles, el sistema d'alerta pràcticament no serveix per a res.

Per tant, sigui del nivell que sigui però especialment si és d'alt nivell, la implantació d'un sistema d'alerta ha d'anar acompanyada de l'estudi de dimensionament i de l'adscripció dels recursos necessaris per garantir la utilitat i l'efectiva atenció, gestió i seguiment de les alertes que el sistema pugui generar.

4.4 Metodologia: del mapa de riscos als elements d'un sistema d'alerta

Arribats a aquest punt del nostre estudi, sembla adient recapitular i sintetitzar les idees, criteris, indicacions i elements metodològics que hem repassat fins aquí.

No es tracta pròpiament d'elaborar una guia metodològica per al disseny i implementació d'un sistema d'alerta, però sí d'establir unes indicacions bàsiques sobre els aspectes principals a tenir en compte.

El punt de partida i premissa principal és la primera de les idees clau apuntades al document *Red Flags for Integrity*: **el context ho és tot**.

Un sistema d'alerta operatiu i eficaç no es dissenya en abstracte, sinó en un determinat context i, per tant, el primer pas metodològic és la **identificació de les alertes rellevants i útils**, de totes les possibles, tenint en compte les especificitats i singularitats de l'organització on es pretengui implementar el sistema d'alertes i del marc legal i operatiu existent.

En aquest primer pas sembla evident que els **òrgans de control intern** han de jugar un rol important: són els que tenen la més acurada i fiable informació i percepció de les febleses i disfuncions de l'organització i de les irregularitats que s'hi han produït, s'hi produeixen i s'hi poden produir. En aquest sentit, l'historial d'objeccions formulats per a la Intervenció constitueix una valuosa font d'informació.

Aquest primer pas consisteix de fet, en gran mesura, en el **procés d'identificació, anàlisi i avaluació dels riscos** que constitueix l'objecte d'una part important dels materials del projecte *Riscos per a la integritat en la contractació pública* de l'Oficina Antifrau, ja esmentat [83]. Per tant, molts dels documents i eines produïts

[83] Cfr. apartat 1.1 anterior (pàg. 6) i nota 1.

en el marc d'aquell projecte seran de gran utilitat per dur a terme correctament aquest primer pas metodològic en el disseny d'un sistema d'alertes.

El segon pas metodològic és **definir cada alerta** concreta, el que comporta diferents operacions conceptuals i organitzatives:

a. per una banda, determinar exactament quina o quines **dades concretes** són necessàries per definir l'alerta, quines són les **relacions lògiques entre les diverses dades** quan siguin més d'una —per aquesta operació serà d'un gran valor el document complementari d'OCP amb el llistat de 73 possibles alertes— i quin o quins són els **valors llindars** de la dada o de cadascuna de les dades que desencadenen l'alerta;

b. d'altra banda, determinar d'on es poden extreure les dades necessàries, és a dir, identificar les diverses **fonts de dades**, tractant de prioritzar l'accés directe a dades de caràcter intern respecte de dades externes —la idea rectora en aquest punt és la ja apuntada de **superioritat dels sistemes interns sobre els externs**, però evidentment això no serà sempre possible—, el que comporta analitzar i avaluar qüestions com la **disponibilitat i qualitat de les dades**, i, quan es tracti de dades personals, les possibilitats del seu tractament atès el règim normatiu aplicable en matèria de **protecció de dades**;

   en aquest punt, el fet de tenir **mapejades les dades d'acord amb l'estàndard OCDS** pot ser útil i convenient des de diversos punts de vista, com ja hem assenyalat, encara que no sigui estrictament necessari;

c. és igualment necessari interpretar correctament el significat de l'alerta, cosa que implica:

   i. associar-la a un concret supòsit o esquema d'**irregularitat, frau o corrupció**;

   ii. determinar la **naturalesa de l'alerta**: si es tracta d'una alerta que dona informació inequívoca sobre l'existència certa d'una irregularitat, frau o corrupció, o d'una alerta que només facilita una informació indiciària sobre la possibilitat —però no la certesa— de l'existència d'una irregularitat, frau o corrupció; i en aquest segon cas, cal determinar si el valor de l'alerta aporta informació sobre la probabilitat, baixa, mitjana o alta de la materialització del risc que es tracti.

Un altre element important d'aquest segon pas metodològic de definició de les alertes concretes del sistema, que té un caràcter continuat en el temps i probablement iteratiu, és la **revisió i millora continua de cada alerta**: una vegada dissenyada i implementada l'alerta, cal analitzar periòdicament i de forma continuada el seu funcionament, per detectar si aquest és correcte i eficaç. Sembla evident que una alerta que genera constants falsos positius, o, al contrari, que pràcticament no salta mai raonablement, o està mal dissenyada o potser no és realment útil: cal determinar per què passa això i dur a terme, si escau, els ajustos adients tant en el disseny mateix de l'alerta com dels valors llindars de la o les dades en què es basa. Idealment, una alerta està òptimament dissenyada i és eficaç quan només salta si realment s'està materialitzant o es pot materialitzar amb total certesa el risc que està dissenyada per detectar.

Un altre pas metodològic, molt proper al que acabem de considerar, és **assignar cada alerta a la corresponent fase del cicle de contractació**, per determinar que el sistema d'alerta —el conjunt d'alertes concretes— cobreix homogèniament tot el cicle de contractació, sense que hi hagi "punts cecs" on es puguin materialitzar els riscos sense que el sistema ho detecti.

Finalment, un últim pas metodològic, molt important, de caràcter organitzatiu, és **definir el tractament i els efectes de l'alerta** i, a aquests efectes, assignar, si escau, els recursos necessaris. Això implica:

a. definir —probablement a nivell normatiu, com a mínim a nivell normatiu intern— els **efectes de l'alerta**: com ja hem vist[84], les possibilitats són molt diverses, i poden anar des del bloqueig total i paralització de la tramitació del procediment fins a simplement la constància en un registre que s'ha produït l'alerta;

b. si l'alerta no és indicativa inequívocament de la materialització efectiva o imminent d'un risc, però només indicativa indiciàriament d'una probabilitat de la mateixa, cal determinar quines **actuacions de verificació o investigació** es duran a terme per confirmar o descartar l'existència, real o potencial del risc, i qui durà a terme aquestes actuacions;

c. igualment, quan l'alerta tingui caràcter purament contingent i, per tant, indiqui la materialització d'un risc, cal definir les actuacions adients per **revertir** —quan sigui possible— **la situació irregular o fraudulenta** produïda, dur a termes les **actuacions disciplinàries i de depuració de responsabilitats** adients i, evidentment, dissenyar i implementar les **mesures de prevenció** necessàries per evitar la perpetuació o reproducció en el futur de la materialització del risc.

Per acabar tractarem de referir de manera concreta aquests elements metodològics a algunes de les alertes corresponents als principals riscos en el cicle de la contractació pública identificats en el document de treball núm. 3 del projecte *Riscos per a la integritat en la contractació pública* de l'Oficina Antifrau[85].

En el quadre de les pàgines següents s'identifiquen alguns d'aquests riscos, seguint l'ordre lògic de les fases del cicle de contractació pública: preparació, licitació, adjudicació i formalització, execució, indicant per cadascun:

---

[84] Cfr. apartat 4.1 anterior (pàg. 60).

[85] Cfr. nota 1 anterior. Aquest document de treball, titulat *Identificació de riscos. 12 àrees de riscos d'irregularitats, frau o corrupció que cal avaluar*, es pot consultar al web de l'Oficina Antifrau a: https://www.antifrau.cat/sites/default/files/Documents/Recursos/DT03_riscos-integritat-contractacio-publica-identificacio-riscos.pdf.

Existeixen moltes i molt diverses taxonomies o classificacions dels riscos de corrupció en el cicle de la contractació pública. La de l'esmentat document de l'Oficina Antifrau és una de les possibles, que coincideix bastant amb la que podem trobar en el document de la OCDE *Analytics for Integrity* —op. cit. apartat 1.2, *Overview of corruption and fraud risks across the infrastructure project cycle* (Resum dels riscos de corrupció i frau en el cicle dels projectes d'infraestructures), pàg. 10 a 13, i annex 1.A, pàg. 20 a 26—. El document *Red Flags for Integrity* utilitza una classificació diferent, basada, com ja hem vist, en la de la *Guia per la lluita contra la corrupció i el frau en els projectes de desenvolupament* (*Guide to Combating Corruption & Fraud in Development Projects*) —cfr. nota 66 anterior—.

a. el risc de què es tracta;

b. la fase del cicle de contractació en la qual es situa;

c. la descripció de la irregularitat concreta i/o del supòsit de frau o corrupció corresponent;

d. la descripció literal de l'alerta;

e. una relació literal de les dades en les quals es basa;

f. la tipologia d'aquestes dades, segons la classificació que ja hem emprat [86]: dades del procediment —en principi directament recopilables del gestor electrònic d'expedients de contractació—, dades de contractació i de comptabilitat de l'entitat contractant, i dades addicionals de caràcter extern: d'altres bases de dades i dades obertes d'Internet;

g. si l'alerta fa ús de dades de caràcter personal;

h. el tipus o naturalesa d'alerta: si dona informació concloent o merament indiciària sobre l'existència d'irregularitats, frau o corrupció;

i. el nivell de l'alerta d'acord amb la tipologia definida a l'apartat 4.3 anterior; i

j. una indicació molt aproximada sobre la complexitat del disseny i implementació de l'alerta, basada principalment en la necessitat d'explotar conjuntament diverses dades per a la mateixa alerta, el tipus de dades i el suport en què es troben —així, a títol d'exemple, l'ús de dades quantitatives o definides inequívocament amb un nombre tancat de possibles valors en camps concrets del gestor d'expedients presenta menys complexitat que l'ús de dades de caràcter textual en documents de l'expedient—.

Destaquem que no s'han inclòs al quadre següent els riscos associats a fets o situacions que, per la seva naturalesa, no tenen, *a priori*, un reflex directe en l'expedient ni, per tant, són susceptibles de datificació, com seria el cas, paradigmàticament, del pagament de suborns o de la filtració d'informacions sobre la contractació a potencials operadors econòmics interessats tant en la fase de preparació com en la de licitació del contracte; o els incompliments o compliments defectuosos de les prestacions, la detecció dels quals requereix verificacions i comprovacions materials, i, per tant, no generen *per se* dades en l'expedient corresponent.

Això no significa que aquests riscos no siguin detectables, però no ho seran directament, sinó indirectament, a través dels seus efectes o conseqüències en tràmits del procediment o situacions del cicle de contractació que sí són susceptibles de datificació i, per tant, de tractament pel sistema d'alerta.

Amb tots aquests elements, tenim el quadre següent:

[86] Cfr. apartat 4.3 anterior (pàg. 63 i seg.).

Risc	Fase de contractació	Irregularitat	Alerta				Tipus	Nivell sistema alerta	Complexitat
			Definició	Dades					
				Identificació	Tipus	Personals			
Existència de situacions de conflicte d'interès	Totes	Presa de decisió o actuació segons criteris no imparcials ni objectius com a conseqüència de la interferència d'un interès particular en conflicte	Detecció de vinculacions entre servidors públics que intervenen en el procediment de contractació i operadors econòmics (participants, licitadors i adjudicatari)	Dades identificadores dels servidors públics que participen directament o indirectament (ascendents jeràrquics o funcionals) en el procediment de contractació. Dades identificadores dels titulars reals / de les persones amb càrrecs de responsabilitat en els operadors econòmics participants / licitadors	Procediment Altres bases de dades (organigrames / RM / titulars reals) Fonts obertes	Sí	Indiciària	2	Mitjana / Alta
Impuls o disseny de contractacions innecessàries, sobredimensionades, o perjudicials	Preparació	Manca de justificació o justificació esbiaixada, inconsistent o incoherent de la contractació	Detecció / comparació amb contractacions antecedents amb el mateix objecte Inexistència de justificació de la contractació Preus no de mercat	Justificació de la contractació Dades de contractacions antecedents Objecte contractual (plecs) Tipus de licitació (plecs) / preus de referència de mercat	Procediment Contractació Altres bases de dades (preus de mercat)	No	Indiciària	2	Mitjana / Alta
Elecció indeguda del procediment	Preparació	Utilització de procediment inadequat / que eludeixi o limiti la competència	Detecció d'inadequació del procediment a les característiques del contracte	Tipus de procediment Justificació del procediment Tipus de licitació (plecs) Objecte contractual (plecs)	Procediment	No	Concloent	0	Baixa
Contractacions amb objectes inconcrets / mal definits	Preparació	Manca de concreció suficient de l'objecte contractual que facilita l'arbitrarietat en la valoració de les ofertes	Detecció d'objecte contractual inconcret / mal definit	Objecte contractual (plecs)	Procediment	No	Indiciària	0	Mitjana
Limitació injustificada de la competència en la licitació	Preparació	Disseny de requisits de participació o de solvència / criteris de selecció qualitativa de participants / licitadors que limitin injustificadament la competència	Detecció de requisits de participació o de solvència / criteris de selecció qualitativa injustificadament restrictius	Requisits de participació o de solvència / criteris de selecció qualitativa de participants / licitadors (plecs)	Procediment	No	Concloent Indiciària	0	Baixa / Mitjana
Abús de subcontractació (per disseny)	Preparació	Facilitar que l'adjudicatari esdevingui *de facto* un poder adjudicador a través de la subcontractació Ocultar situacions de conflicte d'interès o de favoritisme a través de la subcontractació	Detecció d'excés de subcontractació o subcontractació injustificadament restrictiva en el disseny del contracte	Règim de subcontractació (plecs) Dades identificadores dels operadors econòmics que hagin participat en actuacions preparatòries de la contractació Dades per a la detecció de situacions de conflictes d'interès (veure *supra*)	Procediment Contractació Altres bases de dades (RM / titulars reals)	Sí	Concloent Indiciària	2	Mitjana / Alta
Intervenció de licitador (adjudicatari) en el disseny de la contractació / l'elaboració dels plecs	Preparació	Permetre la intervenció directa d'un licitador (previsiblement adjudicatari del contracte) en el disseny de la contractació / l'elaboració dels plecs	Detectar intervencions externes en els treballs de preparació de la contractació	Plecs i documentació de l'expedient de contractació (metadades)	Procediment Altres bases de dades (organigrames / RM / titulars reals)	Sí	Indiciària	2	Mitjana

Risc	Fase de contractació	Irregularitat	Alerta				Tipus	Nivell sistema alerta	Complexitat
			Definició	Dades					
				Identificació	Tipus	Personals			
Criteris de valoració d'ofertes inconcrets / mal definits	Preparació	Disseny de criteris de valoració de les ofertes inconcrets / mal o poc definits que facilitin l'arbitrarietat en la valoració de les ofertes	Detecció de criteris de valoració de les ofertes inconcrets / mal definits	Criteris de valoració d'ofertes i regles / procediments per a la seva aplicació (plecs)	Procediment	No	Concloent Indiciària	0	Baixa / Mitjana
Fraccionament	Preparació / Adjudicació	Fraccionament de l'objecte contractual per eludir procediments amb publicitat i concurrència	Detecció d'acumulació en un mateix adjudicatari de múltiples contractes en un període curt de temps amb objecte idèntic / semblant	Objecte contractual (plecs) Adjudicatari Dades de contractacions antecedents	Procediment Contractació / comptabilitat	Sí	Indiciària	1	Baixa
Asimetria de la informació en la licitació	Licitació	Creació de dèficits o asimetries en la informació facilitada als participants / licitadors	Detecció d'anomalies en la posada a disposició dels operadors econòmics interessats de la informació de la licitació	Publicacions de la licitació	Procediment	No	Indiciària	0	Baixa / Mitjana
Incompliment dels terminis mínims de licitació	Licitació	Falsejament de la lliure concurrència reduint indegudament el termini per a la presentació d'ofertes	Detecció de termini de presentació d'ofertes indegudament curt	Termini de presentació d'ofertes (plecs / publicacions de la licitació)	Procediment	No	Concloent Indiciària	0	Baixa
Pràctiques col·lusòries	Licitació	Falsejament de la lliure concurrència mitjançant col·lusió entre els licitadors (amb o sense coneixement / consentiment de l'ens contractant)	Detecció de pràctiques col·lusòries a través de múltiples indicadors, entre d'altres: - licitador únic; - única oferta admissible; - reiteració dels mateixos licitadors amb estructures d'ofertes anàlogues / adjudicacions rotatòries; - estructura anormal de baixes; - presentació d'ofertes per operadors vinculats	Dades identificadores dels participants / licitadors i dels titulars reals / de les persones amb càrrecs de responsabilitat en els operadors econòmics participants / licitadors Característiques de les ofertes (baixes / altres elements de les ofertes) Participant / licitadors inadmesos	Procediment Contractació Altres bases de dades (RM / titulars reals)	Sí	Indiciària	2	Alta
Admissió o exclusió indeguda de participants / licitadors	Licitació	Admissió o exclusió indeguda de participants / licitador que comporten alteració del principi d'igualtat de tracte i falsegen la competència	Detecció d'admissions o exclusions irregulars de participants / licitadors	Requeriments de solvència / criteris de selecció qualitativa de participants / licitadors i règim d'ofertes anormals (plecs) Aplicació dels criteris de selecció qualitativa de participants / licitadors (informes del procediment) Inadmissió d'ofertes (informes de la licitació) Aplicació irregular del règim d'ofertes anormals (informes de la licitació)	Procediment	No	Concloent Indiciària	0	Mitjana

Risc	Fase de contractació	Irregularitat	Alerta				Tipus	Nivell sistema alerta	Complexitat
			Definició	Dades					
				Identificació	Tipus	Personals			
Valoració irregular / esbiaixada de les ofertes	Adjudicació	Aplicar irregularment / esbiaixadament o modificar els criteris de valoració de les ofertes de forma que s'afavoreixi i/o perjudiqui determinats licitadors	Detecció d'irregularitats en l'aplicació dels criteris de valoració d'ofertes	Criteris de valoració d'ofertes i regles / procediments per a la seva aplicació (plecs) Aplicació dels criteris de valoració d'ofertes (informes de la licitació / d'adjudicació) Existència / composició del comitè d'experts quan sigui preceptiu (art. 146.2 a) LCSP: criteris depenent d'un judici de valor amb ponderació superior a criteris automàtics) Dades identificadores dels integrants del comitè d'experts quan sigui preceptiu	Procediment Altres bases de dades	Sí	Concloent Indiciària	2	Mitjana / Alta
Adjudicació a licitador que no ha presentat millor oferta	Adjudicació	Adjudicar el contracte a un licitador que no és el que ha presentat la millor oferta Apartar-se injustificadament de la proposta d'adjudicació de la mesa de contractació	Detecció d'adjudicació a licitador diferent del proposat / del que ha obtingut la millor puntuació	Aplicació dels criteris de valoració d'ofertes (informes de la licitació / d'adjudicació) Proposta d'adjudicació Resolució d'adjudicació	Procediment	No	Concloent Indiciària	0	Baixa / Mitjana
Irregularitats en els recursos	Licitació / Adjudicació	No tramitar / no resoldre / resoldre irregularment els recursos que puguin presentar els participants / licitadors	Detecció de recursos no tramitats / no resolts / irregularment resolts	Recursos presentats Recursos resolts Sentit / motivació / racionalitat de la resolució	Procediment	No	Concloent	0	Mitjana / Alta
Desistiment injustificat del procediment de contractació	Licitació / Adjudicació	Desistir injustificadament del procediment de contractació	Detecció de desistiment injustificat del procediment de contractació	Resolució de desistiment del procediment de contractació: motivació / racionalitat	Procediment	No	Concloent Indiciària	0	Mitjana
Irregularitats en la formalització del contracte	Adjudicació	Formalitzar el contracte amb l'adjudicatari fora dels terminis establerts / amb alteracions o modificacions respecte de les previsions dels plecs / amb condicionaments no previstos etc.	Detecció de formalització en data anormal Detecció de discordances entre el document de formalització i les previsions dels plecs	Data de formalització Document de formalització Plecs	Procediment	No	Concloent Indiciària	0	Mitjana
Incompliments de terminis contractuals	Execució	Incompliment per part del contractista dels terminis parcials o total per a l'execució del contracte	Detecció de superació de terminis parcials o total del contracte sense que consti l'execució de les prestacions executades	Terminis contractuals, parcials o total (plecs) Documentació d'execució (informes / factures conformades)	Procediment	No	Indiciària	0	Baja
Increments de preus irregulars o no justificats	Execució	Acceptar revisions de preus o preus contradictoris irregulars, no justificats o excessius	Detecció / comparació amb contractacions antecedents amb el mateix objecte Inexistència de justificació de la revisió de preus / preus contradictoris Preus no de mercat	Justificació de la revisió de preus / preus contradictoris (plecs / informes d'execució) Dades de contractacions antecedents Preus de referència de mercat	Procediment Contractació Altres bases de dades (preus de mercat)	No	Indiciària	2	Mitjana / Alta

Risc	Fase de contractació	Irregularitat	Alerta				Tipus	Nivell sistema alerta	Complexitat
			Definició	Dades					
				Identificació	Tipus	Personals			
Modificacions irregulars del contracte	Execució	Modificació del contracte fora dels supòsits legalment admesos, que n'alterin el contingut o elements essencials o que haurien permès l'adjudicació a d'altres participants / licitadors	Detecció de modificacions que incompleixin les limitacions quantitatives (prestacions / preu), qualitatives (previsions en els plecs) o temporals legal o contractualment establertes	Justificació de les modificacions (informes d'execució) Característiques modificacions Resolucions de modificació	Procediment	No	Concloent Indiciària	0	Mitjana
Continuïtat irregular de l'execució de contractes amb termini finalitzat	Execució	Continuar fora dels supòsits legalment admesos l'execució per via de fet (prestacions i pagament) d'un contracte el termini del qual ha finalitzat	Detecció de l'execució de prestacions més enllà de la data de finalització del contracte	Data de finalització Documentació d'execució (informes / factures / etc.)	Procediment	No	Concloent Indiciària	0	Baixa / Mitjana
Adjudicar sense publicitat ni concurrència contractes complementaris	Adjudicació / Execució	Adjudicar a l'adjudicatari d'un contracte d'altres contractes complementaris fora dels casos legalment admesos	Detecció de l'adjudicació de contractes complementaris	Resolucions d'adjudicació de contractes complementaris Dades identificadores de l'adjudicatari Justificació dels contractes complementaris	Procediment Contractació	Sí	Indiciària	1	Mitjana
Pagaments indeguts	Execució	Aprovar pagaments indeguts (avançaments indeguts; pagaments duplicats; facturació de prestacions no executades / no clarament identificades / indegudes; etc.)	Detecció d'incoherències / contradiccions entre les factures presentades i pagaments acordats i les previsions econòmiques del contracte	Documentació i dades d'execució (informes / factures) Resolucions d'aprovació de factures i pagaments Dades econòmiques del contracte (plecs / adjudicació / formalització)	Procediment	No	Concloent	0	Baixa
Abús de subcontractació (en execució)	Licitació / Execució	Irregularitats en la subcontractació:	Detecció: - d'excés de subcontractació / subcontractació no admesa; - subcontractació de licitadors no adjudicataris o operadors que han participat en actuacions preparatòries de la contractació	Documentació i dades d'execució (subcontractació) Dades identificadores del/s subcontractista/es (constància en principi en oferta)	Procediment Contractació	Sí	Concloent Indiciària	1	Mitjana
Subrogació irregular del contractista	Execució	Aprovar la subrogació d'un altre operador en la posició del contractista quan no ho permetin els plecs o el règim legal o això comporti l'alteració sobrevinguda dels requeriments de solvència / criteris de selecció qualitativa de participants / licitadors	Detecció de subrogació d'altres operadors en la posició del contractista / característiques del subrogat	Documentació i dades d'execució (subrogació) Dades identificadores del subrogat Règim de subrogació (plecs) Requeriments de solvència / criteris de selecció qualitativa de participants / licitadors (plecs)	Procediment	Sí	Concloent Indiciària	0	Mitjana / Alta

5 Conclusions i recomanacions

5.1 Conclusions

D'acord amb tot el que s'ha exposat fins aquest punt es poden formular les conclusions següents:

Primera. Els **sistemes automatitzats d'alerta** són un **element essencial en qualsevol sistema d'integritat**. És previsible —i, en tot cas, seria altament desitjable— que aquests tipus de sistemes tinguin un desenvolupament i creixement molt rellevant en els propers anys en la mesura que s'ha demostrat que constitueixen una de les eines més potents i eficaces en la prevenció, detecció, correcció i persecució d'irregularitats i de situacions de frau i de corrupció.

L'estat de situació actual tant en la Generalitat de Catalunya com en l'àmbit local, no permet ser optimista. Es constata que, tot i els grans avanços duts a terme en la digitalització del sector públic i, concretament, en la implementació de solucions per a la tramitació electrònica dels procediments de contractació, el desenvolupament de sistemes automatitzats d'alerta no sembla una prioritat i només s'ha concretat en casos ultraminoritaris.

Es constata doncs **un dèficit significatiu** en el sector públic català a l'hora de treure profit i **explotar totes les potencialitats de la datificació de la contractació pública al servei de la integritat**. El mandat general de servei amb objectivitat els interessos generals, que obliga tots els poders públics i que implica que tota la seva activitat es trobi sotmesa al principi d'integritat, hauria de comportar l'adopció de totes les mesures necessàries per redreçar aquesta situació els propers anys.

Segona. El context actual presenta factors molt favorables al desenvolupament i la implantació efectiva de sistemes automatitzats d'alerta en tant que:

a. es constata una extensió de la datificació de l'activitat del sector públic a mesura que es generalitza la implantació de solucions tècniques per a la tramitació electrònica dels procediments especialment en l'àmbit de la contracció pública; i

b. els fons NextGenerationEU aportaran previsiblement un gran volum de recursos econòmics per al desenvolupament de projectes en l'àmbit que ens ocupa i, a més a més, imposen uns requisits i exigències d'integritat que haurien de generalitzar-se a tota la contestació pública —i no només a aquella part finançada amb fons europeus— i perpetuar-se més enllà de la finalització d'aquell programa europeu, esdevenint un element estructural del nostre marc legal i de gestió de la contractació pública.

Tercera. Tots els desenvolupaments digitals i projectes del sector públic que, aprofitant aquella finestra d'oportunitat, contribueixin al desenvolupament de la digitalització del sector públic i de la seva activitat haurien d'incorporar el

principi d'*integritat per disseny* en la seva concepció i implementació i, per tant, incorporar mecanismes de detecció i prevenció de riscos per a la integritat, no com una opció complementària sinó com un element integrant de l'estructura principal vertebradora de tota solució tecnològica, especialment en l'àmbit de la contractació pública.

Quarta. No existeix un únic sistema d'alerta aplicable a qualsevol organització o entitat contractant. En aquest àmbit el context ho és tot i, per tant, el primer pas metodològic serà la **identificació de les alertes rellevants i útils**, de totes les possibles, tenint en compte les especificitats de l'organització on es pretengui implementar el sistema d'alerta i del marc legal i operatiu existent.

Aquest primer pas consisteix en el **procés d'identificació, anàlisi i avaluació dels riscos** que constitueix l'objecte d'una part important dels materials del projecte *Riscos per a la integritat en la contractació pública* de l'Oficina Antifrau i, per tant, molts dels documents i eines produïts en el marc d'aquell projecte són de gran utilitat en aquesta fase inicial del disseny d'un sistema d'alertes.

Cinquena. La **disponibilitat i qualitat de les dades** de què es nodreixen els sistemes d'alerta constitueixen un element clau de la seva eficàcia. Des d'aquest punt de vista, la **superioritat dels sistemes interns** és indiscutible.

Cal doncs centrar els esforços en el desenvolupament de sistemes d'alerta de caràcter intern, que es nodreixin de dades directament obtingudes dels gestors electrònics d'expedients i es dissenyin amb capacitat per interactuar automatitzadament amb aquests per garantir l'efecte realment preventiu de les alertes.

Sisena. D'altra banda cal no oblidar que els sistemes d'alerta són abans de res eines al servei de les instàncies de control intern sens perjudici de la seva igualment innegable utilitat per al òrgans de control extern i fins i tot al servei de la transparència i de la rendició de comptes.

La participació dels òrgans de control intern en el disseny i implementació dels sistemes d'alerta és doncs necessària i essencial.

Setena. La potència i eficàcia d'un sistema d'alertes ve determinada en gran mesura per la quantitat i qualitat de les fonts de dades que faci servir. En aquest sentit els referents més avançats en l'àmbit que ens ocupa, l'eina Arachne de la Comissió Europea i el sistema SALER de la Comunitat Valenciana fan servir dades de tres grans categories de fonts:

a. dades del gestor electrònic d'expedients de contractació, referides al procediment concret que s'està tramitant;
b. dades de contractació i de comptabilitat de l'ens contractant; i
c. dades addicionals de caràcter extern, tant de registres o bases de dades públics com, amb les degudes cauteles i garanties en matèria de protecció de dades personals, dades obertes d'Internet.

Vuitena. El respecte de les limitacions i garanties derivades del marc legal europeu i nacional en matèria de protecció de dades personals constitueix un element clau que no pot ser negligit en el disseny i implementació de qualsevol sistema d'alerta basat en dades.

Es detecta la necessitat de millorar les previsions i disposicions del marc legal nacional per donar cobertura a sistemes d'alertes més potents i eficaços.

Novena. Dissenyar i implementar un sistema d'alerta sense preveure els **recursos materials, personals i operatius necessaris per a gestionar, verificar i fer el seguiment de les alertes generades** i aprofitar al màxim totes les potencialitats d'un sistema d'aquest tipus és un malbaratament de recursos públics.

Un sistema automatitzat d'alertes és un instrument al servei de la integritat, i la mesura de la seva utilitat és la seva efectivitat. Per tant, tan important com disposar d'un sistema d'alertes és definir clarament el tractament i efectes de les alertes que generi i garantir l'adscripció dels recursos adients per assegurar l'efectivitat real de totes les seves potencialitats.

5.2 Recomanacions i consideracions

Ateses aquestes conclusions generals del present estudi, i d'acord amb allò que preveu l'art. 3 c) de la Llei 14/2008, del 5 de novembre, de l'Oficina Antifrau de Catalunya, es considera adient la formulació de les següents recomanacions i consideracions.

5.2.1 Al Departament d'Economia i Hisenda de la Generalitat de Catalunya, i, específicament, a la Direcció General de Contractació Pública i a la Intervenció General; i al Departament de la Vicepresidència i de Polítiques Digitals i Territori

Primera. L'Administració de la Generalitat de Catalunya i tots els ens instrumentals que integren el seu sector públic han d'aprofundir i avançar en la digitalització i la datificació de la seva activitat, aprofitant especialment els recursos i els imperatius d'integritat dels fons NextGenerationEU, i dotar-se de sistemes automatitzats d'alerta basats en l'explotació i anàlisi de dades.

En aquest sentit, seria desitjable dissenyar, desenvolupar i implantar en el GEEC 2.0 i, si escau, en el TEEC aquest tipus de sistema d'alerta, a més de generalitzar l'ús del GEEC i del TEEC a tot el sector públic de la Generalitat.

El disseny, desenvolupament i implantació en el GEEC i en el TEEC de sistemes automatitzats d'alerta hauria de dur-se a terme amb la participació de la Intervenció General i del CTTI, i amb la col·laboració de la Sindicatura de Comptes i de l'Oficina Antifrau.

Segona. L'ús de dades personals pels sistemes automatitzats d'alerta ha de ser plenament compatible i conforme amb el marc legal vigent europeu i nacional en matèria de protecció de dades.

En aquest sentit, seria desitjable estudiar i, en la mesura que sigui necessari, dur a terme les modificacions i adaptacions normatives adients per tal de garantir que el tractament de dades personals per garantir la integritat en la contractació pública tingui la condició de tractament per obligació legal, interès públic o exercici de poders públics, d'acord amb allò que disposen l'art. 8 de la LOPDGDD i l'art. 6 del RGPD.

Tercera. En qualsevol cas, i amb caràcter general, qualsevol desenvolupament tecnològic de la Generalitat de Catalunya i del CTTI hauria de regir-se pel **principi d'*integritat per disseny*** en la seva concepció i implementació i, per tant, incorporar mecanismes de detecció i prevenció de riscos per a la integritat com un element integrant de l'estructura principal vertebradora de tota solució tecnològica, especialment en l'àmbit de la contractació pública.

5.2.2 Al Consorci Localret.

Quarta. El Consorci Localret ha iniciat el procediment per a la conclusió d'un acord marc per a l'adquisició d'una solució informàtica per al seguiment, control i planificació dels contractes públics dels ens locals, segons els resultats de la consulta preliminar de mercat prèviament duta a terme.

Tot reconeixent el gran valor i utilitat per a tots els ens locals d'aquesta iniciativa, seria desitjable que en el procediment de negociació per a la conclusió d'aquell acord marc i en el subsegüent procés de desenvolupament d'aquella eina es contemplés la incorporació com a element essencial les principals funcionalitats corresponent a un sistema d'alertes per a la integritat en les diverses fases del cicle de contractació pública.

Cinquena. Així mateix, i amb caràcter general, es recomana al Consorci Localret que qualsevol desenvolupament tecnològic que pugui impulsar en el futur es regeixi per l'esmentat **principi d'*integritat per disseny*** en la seva concepció i implementació.

5.2.3 Al Consorci AOC, als ens locals beneficiaris de fons del PRTR, a les Diputacions Provincials, als Consells Comarcals i a l'Area Metropolitana de Barcelona, a través de la seva Agència de Transparència.

Sisena. Cal aprofitar l'impuls als processos de digitalització i datificació de l'activitat del sector públic local que suposen els programes específics amb aquesta finalitat del PRTR finançat amb els fons NextGenerationEU per incorporar sistemes automatitzats d'alerta basats en l'explotació i anàlisi de dades, concebudes, en primera instància —tot i que evidentment amb un abast més ampli—, com a eines al servei de les instàncies de control intern.

Setena. Així mateix, i amb caràcter general, es recomana igualment que qualsevol desenvolupament tecnològic que es pugui dur a terme o impulsar per les entitats destinatàries d'aquestes recomanacions es regeixi per l'esmentat **principi d'*integritat per disseny*** en la seva concepció i implementació.

5.2.4 Al Col·legi de Registradors de la Propietat i Mercantils d'Espanya.

Vuitena. Les dades organitzatives —identificació de les persones representants o titulars de càrrecs de gestió i administració— i de titularitat de les empreses participants als processos de contractació pública són dades clau d'enorme utilitat per a la implementació de nombroses alertes automatitzades en l'àmbit que ens ocupa. Seria per tant desitjable facilitar-ne l'accés automatitzat.

Es sotmet doncs a la consideració del Col·legi de Registradors de la Propietat i Mercantils d'Espanya la conveniència d'estudiar les possibilitats de facilitar l'accés automatitzat a les dades del Registre Mercantil i de Titularitats Reals als sistemes d'alertes que puguin dissenyar i implementar les entitats del sector públic.