



CONSELL DE GARANTIES ESTATUTÀRIES
DE CATALUNYA

**D I C T A M E N 1/2020, de 23 de gener,
sobre el Reial decret llei 14/2019, de 31 d'octubre, pel qual
s'adopten mesures urgents per raons de seguretat pública en
matèria d'administració digital, contractació del sector públic i
telecomunicacions**

El Consell de Garanties Estatutàries, amb l'assistència del president Joan Egea Fernández, del vicepresident Pere Jover Presa, del conseller Jaume Vernet Llobet, del conseller secretari Àlex Bas Vilafranca, dels consellers Francesc de Paula Caminal Badia i Carles Jaume Fernández, de la consellera Margarida Gil Domènech i del conseller Joan Vintró Castells, ha acordat emetre el següent

D I C T A M E N

Sol·licitat per dos grups parlamentaris, respecte del Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions (BOE núm. 266, de 5 de novembre de 2019).

ANTECEDENTS

1. El dia 23 de desembre de 2019 va tenir entrada en el Registre del Consell de Garanties Estatutàries un escrit del president del Parlament, de 20 de desembre (Reg. núm. E2019000693), en què es comunicava al Consell l'Acord de la Mesa del Parlament, de 19 de desembre de 2019, pel qual, segons el que preveuen els articles 16.2.a i 23.f de la Llei 2/2009, de 12 de febrer, del Consell de Garanties Estatutàries (LCGE), es va admetre a tràmit la sol·licitud de dictamen sobre l'adequació a l'Estatut i a la Constitució del Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions, presentada el dia 23 de desembre de 2019, pel Grup Parlamentari de Junts per Catalunya i pel Grup Parlamentari Republicà.

2. En data 30 de desembre de 2019, arran de la gestió realitzada amb els serveis de la Presidència del Parlament, atès que en l'escrit de petició presentat es va observar un error material, en el sentit que li mancaven la meitat de les pàgines, concretament les de nombre parell, es va rebre en el Registre del Consell una carta de la lletrada, per delegació de funcions del secretari general (Resolució de 20 de desembre de 2019), on adjuntava de nou, rectificada, la sol·licitud presentada pels dos grups parlamentaris (Reg. núm. E2019000711), en relació amb el mateix Reial decret llei 14/2019.

Els sol·licitants demanen el dictamen d'aquest Consell, que té caràcter preceptiu segons l'article 76.3 EAC, per al cas que es decidís interposar un recurs d'inconstitucionalitat.

3. El Consell de Garanties Estatutàries, en la sessió del dia 30 de desembre de 2019, d'acord amb els articles 23.b, 24 i 25, apartats 1 a 3, de la Llei 2/2009, de 12 de febrer, després d'examinar la legitimació i el contingut de

la sol·licitud, va acordar la seva admissió a tràmit i es va declarar competent per emetre el dictamen corresponent en el termini d'un mes des de la recepció de la sol·licitud presentada de nou, data a partir de la qual es va poder identificar l'objecte del Dictamen. Igualment, va entendre que no era procedent la seva acumulació amb el Dictamen sol·licitat pel Govern sobre el mateix Reial decret llei, pel fet que ja s'havia enllestit la seva elaboració i, d'acord amb l'ordre del dia, estava prevista la seva votació en la mateixa sessió. Seguidament, es va designar ponent el conseller senyor Jaume Vernet, atesa la connexió directa, per raó del seu objecte, entre la part del Reial decret llei 14/2019 que li va ser assignada com a coponent del Dictamen precedent i les qüestions noves que plantejava la present petició.

4. En la mateixa sessió, a l'empara de l'article 25 LCGE, apartats 4 i 5, i de l'article 35 del Reglament d'organització i funcionament del Consell, va acordar adreçar-se als sol·licitants, a tots els grups parlamentaris i també al Govern a fi de sol·licitar-los la informació i la documentació complementàries de què disposessin sobre la norma sotmesa a dictamen.

5. Finalment, després de les corresponents sessions de deliberació del Consell, el dia 23 de gener de 2020 ha tingut lloc la votació i l'aprovació d'aquest Dictamen, d'acord amb el que preveuen els articles 30.2 LCGE i 38 del Reglament d'organització i funcionament del Consell.

FONAMENTS JURÍDICS

Primer. L'objecte del Dictamen

Tal com consta en els antecedents, aquest Dictamen s'emet per donar resposta a la sol·licitud presentada per dos grups parlamentaris, amb caràcter previ a l'eventual interposició, per part del Parlament, d'un recurs

d'inconstitucionalitat davant del Tribunal Constitucional, a l'empara dels articles 16.2.a i 23.f LCGE, amb relació al Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions (en endavant, RDL 14/2019 o Reial decret llei).

En concret, tot i que en el seu escrit els grups peticionaris no fan una enumeració expressa de preceptes, sí que manifesten dubtes de constitucionalitat i d'estatutarietat, d'una banda, sobre tot el Reial decret llei, pel que fa a la seva adequació a l'article 86.1 CE, i, de l'altra, respecte de la integritat o part dels articles 1, 2, 3.u, .dos i .tres i, per connexió amb aquest darrer article, la disposició transitòria primera, com també l'article 6.u, .dos i la disposició addicional única del Reial decret llei. D'aquesta circumstància podem deduir que són únicament aquests preceptes els que es posen en qüestió i, per tant, sobre els quals es demana la nostra opinió consultiva, de manera que ens cenyirem al seu examen, a excepció de les disposicions finals primera i segona del Reial decret llei que, en la mesura que contenen, respectivament, els títols competencials que fonamenten la norma i l'habilitació per al seu desenvolupament i la seva execució, seran tractades per connexió amb els preceptes anteriors.

En conseqüència, i des del punt de vista del seu contingut material, no seran objecte de la nostra anàlisi els articles 4, 5 i 6, apartats 3 a 5, ni l'article 7, com tampoc les disposicions transitòries segona i tercera i final tercera.

Com a qüestió prèvia, abans de procedir a la determinació de l'objecte del Dictamen, hem de fer avinent que, com s'apunta en els antecedents, el Consell s'acaba de pronunciar sobre aquesta mateixa norma legal en el Dictamen 6/2019, de 30 de desembre, emès a petició del Govern de la Generalitat. En aquesta ocasió, el Reial decret llei va ser analitzat des de la perspectiva de la seva adequació constitucional a l'article 86.1 CE i es va

efectuar l'escrutini de constitucionalitat i estatutarietat dels preceptes següents: articles 1; 2; 3.u i .dos; 4; 6.u, .dos i .cinc, i 7; la disposició addicional única, i, per connexió, les disposicions transitòries primera, apartats 1 i 2; segona, i la disposició final primera. Partirem doncs d'aquest Dictamen per determinar el contingut i l'estructura de la present opinió consultiva, com exposarem tot seguit.

Seguint el mateix tipus de procedir que en el DCGE 6/2019, i per les raons que hi hem indicat, en aquest fonament jurídic només recordarem succintament tant el contingut del Reial decret llei, pel que ara interessa, com també els dubtes expressats pels grups peticionaris en el seu escrit. Així doncs, diferirem la descripció i contextualització dels preceptes, com també el detall dels arguments aportats en la sol·licitud, al moment en què ens hi referim de forma particularitzada, en un cas directament i en els altres per remissió al DCGE 6/2019.

1. El Reial decret llei 14/2019, que ha estat convalidat per l'Acord de la Diputació Permanent del Congrés dels Diputats de 27 de novembre de 2019 (publicat per la Resolució de la Presidència del Congrés de la mateixa data al BOE núm. 291, de 4 de desembre de 2019), consta de set articles, estructurats en cinc capítols, una disposició addicional, tres de transitòries i tres de finals.

Aquests preceptes es refereixen a diversos àmbits materials i modifiquen les respectives normes sectorials, que es concreten en mesures en matèria de documentació nacional d'identitat (cap. I, art. 1 i 2); identificació electrònica davant les administracions públiques, ubicació de determinades bases de dades i dades cedides a altres administracions (cap. II, art. 3 i 4); contractació pública (cap. III, art. 5); seguretat en matèria de telecomunicacions (cap. IV, art. 6, i disp. add. única), i coordinació en

matèria de seguretat de les xarxes i els sistemes d'informació (cap. V, art. 7).

Pel que ara interessa als efectes del Dictamen, i en relació amb les disposicions normatives del Reial decret llei que seran objecte d'examen, els articles 1 i 2 modifiquen, respectivament l'article 8.1 de la Llei orgànica 4/2015, de 30 de març, de protecció de la seguretat ciutadana (en endavant, LOPSC) i l'article 15.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica (en endavant, LSE), en relació amb el document nacional d'identitat i el document nacional d'identitat electrònic.

L'article 3.u i .dos reforma els articles 9.2.c i 10.2.c i afegeix un nou apartat 3 a aquests articles 9 i 10 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (en endavant, LPACAP), quant a les mesures d'identificació i signatura electròniques dels interessats davant les administracions públiques, i la disposició transitòria primera del Reial decret llei, apartat 1, estableix el règim transitori de les modificacions dutes a terme pel precepte esmentat. Per la seva banda, l'apartat tres de l'article 3 afegeix una nova disposició addicional sisena a la LPACAP, relativa a les tecnologies de registre distribuït com a base dels sistemes d'identificació i signatura electròniques.

L'article 6.u dona nova redacció a l'article 4.6 de la Llei 9/2014, de 9 de maig, general de telecomunicacions (en endavant, LGTEL) i el seu apartat dos introdueix un nou apartat 3 a l'article 6 LGTEL, tots dos preceptes referits a les xarxes i els serveis de comunicacions electròniques, l'últim dels quals a les xarxes en règim d'autoprestació de les administracions públiques. En relació amb l'article 6.3 LGTEL, cal afegir l'obligació de comunicació d'aquestes xarxes al Ministeri d'Economia i Empresa que preveu la disposició addicional única del Reial decret llei, quan hagin estat instal·lades o estiguin en procés d'instal·lació o explotació. A l'últim, la disposició final primera

comprèn els títols competencials habilitants dels preceptes del Reial decret llei. Pel que ara interessa, l'article 149.1.29 CE pel que fa als articles 1 i 2; l'article 149.1.18 i .29, quant a l'article 3, i l'article 149.1.21 en relació amb l'article 6 i la disposició addicional única.

2. L'escrit de petició del Dictamen, en primer lloc, qüestiona tota la norma des del punt de vista de la seva constitucionalitat ex article 86.1 CE, atès que postula que no existeix l'extraordinària i urgent necessitat ni una connexió de sentit entre les modificacions legislatives aprovades i el pressupòsit habilitant al·legat pel Govern de l'Estat, per la qual cosa s'envaeix «la potestat legislativa que correspon a les Corts Generals» i, per tant, «el principi de separació de poders». A més a més, els dos grups parlamentaris entenen que la deferència constitucional envers el judici d'oportunitat del Govern de l'Estat no pot ser la mateixa quan es tracta d'un Govern en funcions i no d'un Govern amb plenitud d'atribucions, tenint en compte, a més, la convalidació per part de la Diputació Permanent sense esperar la constitució del nou Congrés dels Diputats, decisió que té «una incidència directa sobre el dret de participació política dels nous diputats electes».

Igualment, els sol·licitants argumenten que el Reial decret llei vulnera, des del punt de vista substantiu, l'àmbit competencial de la Generalitat, com també el principi de seguretat jurídica de l'article 9.3 CE. En aquest sentit, addueixen, en el seu escrit, que els articles 1 i 2 RDL 14/2019, a més de no superar el cànon constitucional de l'article 86.1 CE, amb relació a l'article 101.2 CE, excedeixen les competències de l'Estat de l'article 149.1.18 i .29 CE i contravenen l'article 159 EAC, en la mesura que esgoten la regulació en aquesta matèria i deixen sense cap marge de desenvolupament les comunitats autònomes.

Els dos grups parlamentaris al·leguen la mateixa conculcació de l'article 86.1 CE i dels anteriors preceptes competencials de la Constitució i l'Estatut, pel

que fa a l'article 3.u i .dos del Reial decret llei, en la reforma que efectua dels articles 9.2.c i 10.2.c LPACAP, perquè entenen que la subjecció a l'autorització prèvia de l'Estat dels sistemes d'identificació i de signatura electròniques no basats en certificats electrònics qualificats no pot trobar empara en l'article 149.1.18 ni .29 CE, aquest últim per tal com és injustificat i desproporcionat que aquesta potestat s'atribueixi sobre la base dels riscos que «això pugui comportar per la seguretat pública». Les anteriors consideracions es fan extensives als nous articles 9.3 i 10.3 LPACAP, sobre els quals se sosté que, a més, vulneren la lliure prestació de serveis reconeguda al Tractat de funcionament de la Unió Europea.

Pel que fa a l'apartat tres de l'article 3 del Reial decret llei, els sol·licitants consideren que la nova disposició addicional sisena LPACAP que aquest afegeix, relativa a l'ús dels sistemes d'identificació i signatura basats en tecnologies de registre distribuït, no constitueix una restricció temporal i puntual sinó que suposa una limitació al desenvolupament normatiu en el marc de les bases del procediment administratiu de règim jurídic que reconeix l'article 159 EAC, a part que la indefinició en les funcions que s'atorguen a l'Administració general de l'Estat, a més de vulnerar l'article 149.1.29 CE «per excedir el concepte de seguretat pública establert per la jurisprudència del Tribunal Constitucional», genera una «evident inseguretat jurídica contrària a l'article 9.3 CE». Per la seva connexió amb l'article 3 del Reial decret llei també consideren que la disposició transitòria primera d'aquesta norma vulnera els mateixos preceptes constitucionals i estatutaris.

Els grups peticionaris aporten idèntica justificació sobre la contravenció de l'article 149.1.29 CE en el supòsit de l'apartat u de l'article 6 del Reial decret llei, en la nova redacció que dona a l'apartat 6 de l'article 4 LGTEL, quant a la facultat d'intervenció de les xarxes i els serveis de comunicacions electròniques que s'hi preveu. Així mateix, entenen que vulnera tant l'article 9.3 CE, per l'absoluta indeterminació dels conceptes que empra, com també

les competències de la Generalitat. Per la seva banda, consideren que l'apartat dos de l'article 6 del Reial decret llei, quan afegeix un nou apartat 3 a l'article 6 LGTEL, a més d'excedir l'article 86.1 CE, amb relació a l'article 101.2 CE, perquè és «evident que aquesta mesura no té cap connexió de sentit amb una situació de necessitat extraordinària i urgent», vulnera la competència executiva de la Generalitat reconeguda per l'article 140.7 EAC en matèria de comunicacions electròniques, per tal com «els projectes d'instal·lació i explotació de xarxes de comunicacions electròniques que impulsa la Generalitat tenen per objecte assolir un conjunt mínim de serveis d'accés universal».

3. Per tal de donar resposta a la petició i, com hem dit, tenint present l'emissió del DCGE 6/2019, el nostre pronunciament s'estructurarà de la manera següent:

El fonament jurídic segon es referirà a les qüestions i els preceptes que ja van ser tractats en el Dictamen mencionat, i contindrà una remissió general a l'argumentació que allà es va fer i a la conclusió a la qual es va arribar, de manera que només s'afegirà una nova anàlisi en el supòsit que la sol·licitud plantegi els dubtes des d'una nova perspectiva. Aquest és el cas de la subjecció del Reial decret llei al pressupòsit habilitant de l'article 86.1 CE, amb l'anàlisi del qual iniciarem aquest fonament jurídic.

Per la seva banda, el fonament jurídic tercer es dedicarà a l'únic precepte, dels que són objecte de crítica en l'escrit de sol·licitud, que no va ser tractat en el DCGE 6/2019, és a dir, l'article 3.tres del Reial decret llei que incorpora una nova disposició addicional sisena a la LPACAP. En aquest cas, el seu examen seguirà l'esquema d'anàlisi ordinari dels nostres dictàmens. A aquest article s'afegirà, així mateix, i per connexió, l'examen de les disposicions finals primera, pel que fa a l'habilitació competencial d'aquest precepte, i la disposició final segona de la norma.

Segon. L'examen de constitucionalitat i d'estatutarietat de les qüestions i els preceptes del Reial decret Llei 14/2019 coincidents amb els que van ser objecte del DCGE 6/2019

En els apartats que segueixen ens referirem a les diferents qüestions que suscita la petició de dictamen, amb l'excepció de l'anàlisi de la disposició addicional sisena LPACAP, afegida per l'article 3.tres RDL 14/2019 i altres disposicions que hi estiguin connectades, que tractarem en el fonament jurídic següent, com hem anunciat. Primerament, s'analitza el compliment del pressupòsit habilitant del Reial decret Llei, d'acord amb les dues perspectives que presenta la sol·licitud. Segonament, la documentació acreditativa de la identitat (art. 1 i 2 RDL 14/2019). Tercerament, els sistemes d'identificació i signatura electròniques dels interessats davant de les administracions (art. 3.u i .dos RDL 14/2019, relatiu als art. 9.2.c i 10.2.c LPACAP, i disp. trans. primera.1.1 RDL 14/2019, art. 9.3 i 10.3 LPACAP i disp. trans. primera.2 RDL 14/2019), llevat del que disposa el Reial decret Llei respecte dels que es basen en la tecnologia de registre distribuït (abans esmentada disp. add. sisena). Finalment, s'examinen l'article 6 RDL 14/2019, que modifica la Llei general de telecomunicacions en matèria de xarxes i comunicacions electròniques (art. 4.6 LGTEL i art. 6.3 LGTEL) així com la disposició addicional única RDL 14/2019. Allà on correspongui es faran les remissions al DCGE 6/2019, que ja va resoldre la petició de dictamen presentada pel Govern sobre els mateixos preceptes del Reial decret Llei.

1. La sol·licitud expressa dos tipus de dubtes respecte a l'ús de la figura del decret Llei, tot proposant que tinguin una anàlisi separada.

A) D'una banda, destaca que el Reial decret Llei 14/2019 objecte d'aquest Dictamen «constitueix un ús excessiu, abusiu i arbitrari de la potestat legislativa provisional» del Govern de l'Estat, atribuïda per l'article 86 CE, i

que, en conseqüència, suposa «una vulneració palmària del principi de separació de poders». A més a més, els grups peticionaris, amb citació de la jurisprudència constitucional, indiquen que aquesta ha criticat la utilització de fórmules rituals d'una marcada abstracció.

Sobre aquesta darrera crítica, en la conclusió primera del DCGE 6/2019 hem considerat que els articles 1, 2, 3, 4, 6, 7, les disposicions addicional única i transitòries primera i segona i la disposició final primera del Reial decret llei 14/2019 són contraris a l'article 86.1 CE, perquè no compleixen el requisit constitucional de l'extraordinària i urgent necessitat.

En el fonament jurídic 2.1 del dit DCGE 6/2019 hem fet referència expressa a la inexistència d'una acreditació explícita i raonada, que pogués justificar el compliment de l'extraordinària i urgent necessitat, descartant la virtualitat de les clàusules rituals i abstractes de l'argumentació del Govern estatal en el preàmbul de la norma, a les quals es refereix l'actual petició de dictamen. Addicionalment, en relació amb el principi de separació de poders, hem de dir que aquesta qüestió ja la va tenir en compte el constituent quan va preveure de forma taxada l'eventualitat que el Govern exercís excepcionalment la potestat legislativa, que ordinàriament correspon a les Corts Generals.

B) D'altra banda, fa una segona crítica dirigida al fet que el Govern de l'Estat, que va aprovar el Reial decret llei 14/2019, «va cessar amb la celebració de les eleccions generals del passat 28 d'abril de 2019» i, per tant, és un Govern en funcions.

El mateix escrit de petició de dictamen, a partir de la interpretació de l'article 78.2 CE, reconeix que un govern en funcions pot dictar decrets llei. «Ara bé, això no vol dir que la situació de Govern en funcions, com la situació de dissolució del Congrés dels Diputats en el moment de la convalidació, sigui

irrellevant des del punt de vista constitucional». A partir d'aquesta consideració, arriba a la conclusió que «no es pot passar per alt la rellevància constitucional del fet que el Reial decret llei 14/2019 hagi estat convalidat per la Diputació Permanent el 27 de novembre, sense esperar la constitució del nou Congrés dels Diputats elegit el 10 de novembre, a pesar que quedaven molts dies perquè s'exhaurís el termini de trenta al qual fa referència l'article 86.2 CE». Per tant, segons els grups peticionaris, s'hauria d'esperar, per a l'acte de la convalidació, a la constitució del *nou* Congrés, ja que altrament això té «una incidència directa sobre el dret de participació política dels nous diputats electes, els quals s'han vist privats de la possibilitat de controlar aquesta disposició legislativa».

En relació amb el tema plantejat, s'ha d'indicar que, d'acord amb l'article 101 CE, el Govern cessa després de la celebració d'unes eleccions generals, tot i que aquest Govern cessant continua en funcions fins a la presa de possessió del nou Govern. La figura del Govern en funcions deriva directament del mandat constitucional (art. 101.2 CE) i té la finalitat d'«evitar vacíos de poder y asegurar en todo momento la continuidad del funcionamiento de la Administración y de la acción de Gobierno» (STC 97/2018, de 19 de setembre, FJ 2). Per tant, entre altres cometes, pot dictar reials decrets llei si concorren els requisits exigits per l'article 86.1 CE, cosa que tampoc no critiquen els grups sol·licitants.

La funció de control del Govern correspon a les Corts Generals (art. 66.2 CE) i, tal com declara la doctrina constitucional, que acota el seu abast (STC 124/2018, de 14 de novembre, FJ 4 i 7), «está implícita en su carácter representativo y en la forma de gobierno parlamentario que establece el art. 1.3 CE, no pudiendo negarse a las Cámaras todo ejercicio de la función de control, ya que con ello se afectaría al equilibrio de poderes previsto en nuestra Constitución» (ibídem, FJ 9).

Pel que ara interessa, d'acord amb l'article 78.2 CE, el control d'aquest Govern en funcions l'han d'exercir les diputacions permanents del Congrés de Diputats i del Senat, atès que són les institucions que garanteixen la continuïtat de l'òrgan parlamentari en el període d'inactivitat de la Cambra i les que el substitueixen, tot assumint, ni que sigui de forma limitada, les seves funcions. Per tant, en el cas que les cambres es trobin dissoltes, les diputacions permanents continuaran exercint les seves funcions fins que es constitueixin les noves Corts Generals (art. 78.2 i .3 CE).

Quant al control de la potestat legislativa del Govern, la Diputació Permanent del Congrés assumeix la facultat de convalidar o derogar els reials decrets llei (art. 78.2 i 86.2 CE).

De fet, no ha estat inusual que la Diputació Permanent del Congrés, un cop celebrades les eleccions generals i atès que no s'havia constituït encara la nova Cambra, convalidés diversos reials decrets llei. Així ho va fer el 24 de juny de 1986, en la II legislatura; el 23 de juny de 1993 se'n convalidaren cinc de la IV legislatura, i el 25 de març de 1996 se'n va convalidar un altre de la V legislatura.

Altrament, pel que fa a l'exercici dels drets de participació dels diputats, concretament al dret de control dels parlamentaris sobre les activitats del Govern, fins que no es constitueixen les noves cambres i s'inicia la següent legislatura correspon als diputats membres de la Diputació Permanent del Congrés, que són els que tenen atribuïda la funció de convalidar o derogar els reials decrets llei (art. 78.2 CE), per a la qual disposen del termini de trenta dies des de la promulgació de la norma (art. 86.2 CE).

Centrant-nos en el cas que ens ocupa, es van convocar eleccions el 28 d'abril i el 10 de novembre de 2019; el Govern en funcions va aprovar el Reial decret llei 14/2019 el 31 d'octubre de 2019 i va ser promulgat i publicat el

dia 5 de novembre de 2019; la Diputació Permanent del Congrés va celebrar l'acte de convalidació el 27 de novembre de 2019, dins dels trenta dies previstos constitucionalment, i les noves cambres es van constituir el 3 de desembre de 2019.

En conseqüència, es compleixen els requisits constitucionals perquè la Diputació Permanent del Congrés dels Diputats de la legislatura en curs hagi pogut controlar el Reial decret llei 14/2019 dins del termini constitucionalment establert, sense que això vulneri els drets de participació dels diputats electes, en tant que no s'havia constituït el nou Congrés.

2. Documentació d'identitat. Articles 1 i 2 del Reial decret llei.

Segons la sol·licitud de dictamen, la literalitat de l'article 1 RDL 14/2019 sobre el caràcter únic del document nacional d'identitat implica de forma principal que, «inexcusablement, la creació de sistemes d'identificació i signatura haurà d'anar precedida d'una identificació personal que només podrà acreditar-se mitjançant el document nacional d'identitat», cosa que constitueix un excés de les competències estatals previstes en els números 18 i 29 de l'article 149.1 CE i una vulneració de l'article 159 EAC. A aquestes mateixes consideracions sotmet la petició l'article 2 RDL 14/2019, en relació amb el document nacional d'identitat electrònic.

D'acord amb la conclusió sisena del DCGE 6/2019, aquests dos preceptes del Reial decret llei no són contraris a l'Estatut ni a la Constitució, en virtut del que s'exposa en el seu fonament jurídic 3.1, al qual ens remetem.

3. Sistemes d'identificació. Article 3, apartats u i dos, i disposició transitòria primera del Reial decret llei.

A) Articles 9.2.c i 10.2.c de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques i disposició transitòria primera, apartat 1, RDL 14/2019

Respecte als articles 9.2.c i 10.2.c LPACAP, modificats pels apartats u i dos de l'article 3 RDL 16/2019, relatius als sistemes d'identificació i de signatura electròniques dels interessats davant les administracions públiques, els grups sol·licitants critiquen els primers des del vessant competencial, entenent que l'autorització estatal prèvia que s'hi preveu, vulnera l'article 159 EAC, sense estar emparada aquesta extralimitació per l'article 149.1.18 i .29 CE. Per connexió, consideren que s'hauria de tractar igualment la disposició transitòria primera RDL 14/2019.

Amb relació a aitals preceptes, en la conclusió segona del DCGE 6/2019 hem afirmat que l'incís, «amb l'autorització prèvia de la Secretaria General d'Administració Digital del Ministeri de Política Territorial i Funció Pública, que només es pot denegar per motius de seguretat pública, amb l'informe previ vinculant de la Secretaria d'Estat de Seguretat del Ministeri de l'Interior. L'autorització s'ha d'emetre en el termini màxim de tres mesos. Sense perjudici de l'obligació de l'Administració General de l'Estat de resoldre dins del termini, la manca de resolució de la sol·licitud d'autorització s'entén que té efectes desestimatis», previst en els articles 9.2.c i 10.2.c LPACAP, «vulnera les competències de la Generalitat de l'article 159 EAC i no troba empara en l'article 149.1.18 i .29 CE». L'argumentació d'aquesta decisió la trobem en el fonament jurídic 3.2 del DCGE 6/2019, al qual ens remetem.

Per connexió i pels mateixos motius, «la disposició transitòria primera, apartat 1, i la disposició final primera, apartat 2, del Reial decret llei 14/2019 també les vulneren i tampoc no troben empara en els preceptes constitucionals citats», segons exposem en el DCGE 6/2019, fonament jurídic 3.2.D.

B) Articles 9.3 i 10.3 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques i disposició transitòria primera, apartat 2, RDL 14/2019

Pel que fa als articles 9.3 i 10.3 LPACAP, afegits pels apartats u i dos de l'article 3 RDL 14/2019, dins de sistemes d'identificació i de signatura electròniques, en relació amb la ubicació i la transferència de les dades a un tercer país o organització internacional, la sol·licitud de dictamen també els critica des del vessant competencial, entenent que vulneren l'article 159 EAC i no troben empara en l'article 149.1.29 CE, a banda de vulnerar la llibertat de prestació de serveis reconeguda en el Tractat de funcionament de la Unió Europea. Consideren que, per connexió, també s'hauria de tractar la disposició transitòria primera.2 RDL 14/2019.

Sobre això, la conclusió cinquena del DCGE 6/2019 diu que els articles 9.3 i 10.3 LPACAP, en l'obligació «de situar "en territori espanyol" els recursos tècnics necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió dels sistemes previstos en els articles 9.2.c i 10.2.c LPACAP, com també, per connexió, la disposició transitòria primera.2 RDL 14/2019, són contraris al principi de lliure circulació de dades previst a l'article 1 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, quant al tractament de dades personals i a la lliure circulació d'aquestes i pel qual es deroga la Directiva 95/46/CE». L'argumentació que fonamenta aquesta decisió la trobem en el fonament jurídic 5.2 del DCGE 6/2019, al qual ens remetem.

4. Xarxes i comunicacions electròniques. Article 6, apartats u i dos i disposició addicional única del Reial decret llei.

A) Article 4.6 de la Llei 9/2014, de 9 de maig, general de telecomunicacions

La petició de dictamen qüestiona que l'Administració de l'Estat, en virtut de la modificació de l'article 4.6 LGTEL per l'article 6.u RDL 14/2019, pugui, excepcionalment i transitòria, sense intervenció judicial, intervenir xarxes i serveis de comunicacions electròniques, fonamentant-ho en l'article 149.1.29 CE.

Segons els sol·licitants, l'«absoluta indeterminació dels conceptes que empra el nou article 4.6 LGTEL vulnera l'article 9.3 CE» i, en la mesura que els serveis de comunicació electrònica siguin instrumentals per a l'exercici de les competències de la Generalitat, també les vulnera.

En la conclusió tercera del DCGE 6/2019 hem considerat que l'article 6.u del Reial decret llei 14/2019, «en la redacció que dona al primer paràgraf de l'apartat 6 de l'article 4 de la Llei 9/2014, de 9 de maig, general de telecomunicacions, quant a la facultat d'«intervenció» que atribueix a l'Estat, és inconstitucional perquè vulnera l'article 9.3 CE, ja que no compleix les exigències de qualitat normativa que hauria d'observar una llei susceptible de produir ingerències en l'exercici dels drets fonamentals i les llibertats públiques», d'acord amb els arguments que es detallen en el fonament jurídic 4.2.C del dit Dictamen, al qual ens remetem.

B) Article 6.3 de la Llei 9/2014, de 9 de maig, general de telecomunicacions i disposició addicional única del RDL 14/2019

Finalment, els grups parlamentaris qüestionen l'examen del nou article 6.3 LGTEL, introduït per l'article 6.dos RDL 14/2019, com també de la disposició addicional única d'aquesta norma. Aquests preceptes tracten de la comunicació al Ministeri d'Economia i Empresa de les instal·lacions en règim d'autoprestació que facin ús del domini públic. Concretament, la petició parteix de la incardinació material de la regulació en l'article 149.1.21 CE,

però, en tant que els projectes de les instal·lacions i l'explotació de les xarxes de comunicació electròniques que impulsa la Generalitat tenen per objecte assolir un conjunt mínim de serveis d'accés universal, la seva acció es troba emparada per l'article 140.7 EAC.

D'acord amb la conclusió sisena del DCGE 6/2019, aquests dos preceptes del Reial decret llei 14/2019 «no són contraris a l'Estatut ni a la Constitució», en virtut del que s'exposa en el seu fonament jurídic 4.3, al qual ens remetem.

Tercer. L'examen de constitucionalitat i d'estatutarietat sobre l'article 3.tres del Reial decret llei 14/2019

A continuació, procedim a revisar la nova disposició addicional sisena LPACAP, en la redacció prevista per l'apartat tres de l'article 3 del Reial decret llei, la qual està directament connectada i ha de situar-se en el context del que disposen els articles 9 i 10 LPACAP, reformats també pels precedents apartats u i dos del mateix article 3. En concret, la disposició ara analitzada conté una regulació que afecta de manera significativa els sistemes d'identificació i de signatura electròniques dels interessats en el procediment administratiu a què fan referència els apartats 2.c dels citats articles 9 i 10 (sistemes de clau concertada i altres que comptin amb un registre previ com a usuari que permeti garantir la seva identitat) quan es basin en la tecnologia de registre distribuït. Els dits preceptes han estat tractats en el fonament jurídic 3.2 del DCGE 6/2019.

Pel que fa a la disposició addicional sisena, se seguirà, com hem avançat, el mètode ordinari d'anàlisi dels dictàmens, és a dir, es descriurà el seu contingut i s'enquadrarà en el context normatiu corresponent, es recolliran els dubtes que planteja la sol·licitud i s'elaborarà el cànon de constitucionalitat i estatutarietat per, seguidament, aplicar-lo al precepte

concret per dilucidar si presenta o no targes d'inconstitucionalitat i d'antiestatutarietat.

De forma literal, la dita disposició addicional estableix que:

«Disposició addicional sisena. Sistemes d'identificació i signatures previstos als articles 9.2 c) i 10.2 c).

1. No obstant el que disposen els articles 9.2 c) i 10.2 c) d'aquesta Llei, en les relacions dels interessats amb els subjectes sotmesos a l'àmbit d'aplicació d'aquesta Llei no són admissibles en cap cas, i per tant no es poden autoritzar, els sistemes d'identificació basats en tecnologies de registre distribuït i els sistemes de signatura basats en els anteriors, mentre no siguin objecte d'una regulació específica per part de l'Estat en el marc del dret de la Unió Europea.

2. En tot cas, qualsevol sistema d'identificació basat en la tecnologia de registre distribuït que prevegi la legislació estatal a què fa referència l'apartat anterior ha d'establir així mateix que l'Administració General de l'Estat actua com a autoritat intermèdia que exerceix les funcions que correspongui per garantir la seguretat pública.»

1. Els sol·licitants consideren que aquesta norma no permet a l'Administració de la Generalitat desenvolupar sistemes d'identificació i de signatura electròniques basats en tecnologies de registre distribuït i que això limita el «desenvolupament normatiu en el marc de les bases del procediment administratiu de règim jurídic que reconeix l'article 159 EAC».

A parer seu, la falta de determinació de les bases per part de l'Estat i la manca d'exercici de la Unió Europea de les seves competències no pot impedir l'ús de les competències legislatives autonòmiques i, per tant, no és constitucionalment admissible «assolir aquest objectiu mitjançant l'establiment d'unes bases que consisteixin [...] a prohibir a les comunitats autònomes l'exercici de la seva potestat legislativa mentre l'Estat no reguli

un determinat àmbit [...] quan ni tan sols es determina un termini per a desenvolupar aquestes bases».

Així mateix, els grups peticionaris critiquen la no concreció de les funcions que correspondrien a l'Administració estatal com a autoritat intermèdia, circumstància que vulneraria l'article 149.1.29 CE en excedir el concepte de seguretat pública establert en la jurisprudència constitucional i, a més, provocaria una inseguretat jurídica contrària a l'article 9.3 CE.

La contravenció dels esmentats preceptes, constitucionals i estatutaris, es predica també, per la seva connexió, de la disposició transitòria primera RDL 14/2019.

2. La nova disposició adicional sisena LPACAP incorpora la primera referència legislativa en l'ordenament jurídic espanyol a les tecnologies de registre distribuït (TRD), en anglès *distributed ledger technologies*.

El registre distribuït es defineix com una tecnologia que es fonamenta en una base de dades digital descentralitzada en la qual existeixen còpies de la informació distribuïdes entre diversos participants que són actualitzades de forma sincronitzada i per acord dels usuaris. Així, l'actualització es realitza de forma consensuada i sense la intermediació d'una autoritat central, a diferència dels sistemes de bases de dades centralitzades.

L'Organització Internacional de Normalització (*International Organization for Standardization —ISO—*), en els treballs d'estandardització que està realitzant (*ISO/DIS 22739 Blockchain and distributed ledger technologies—Terminology*, elaborada pel Comitè Tècnic ISO 307 *Blockchain and distributed ledger technologies*), ha definit la *distributed ledger technology* com la tecnologia que permet l'operació i l'ús de registres distribuïts, entesos com a magatzems d'informació que conserven registres finals, definitius i

inmutables de transaccions que es comparteixen i se sincronitzen de forma descentralitzada i utilitzant mecanismes de consens. Convé precisar també que, en aquest context, el terme «transacció» es refereix a la unitat més petita d'un procés de treball relatiu a les interaccions amb la tecnologia esmentada.

En general, les característiques comunes atribuïdes a les diverses TRDs, sens perjudici dels matisos que deriven de la configuració concreta de cada xarxa, són: la descentralització dels nodes que registren la informació; la confiança i transparència, atès que tots els participants poden veure les operacions que es realitzin i verificar-ne la validesa, tot i que no implica que sempre puguin identificar-ne l'autor; la traçabilitat i integritat de la informació incorporada, i la seva irrevocabilitat i immutabilitat, de manera que la informació registrada no es pot modificar.

Entre els sistemes TRD hom pot distingir, a grans trets, entre els públics i els privats segons els requisits d'accés dels seus participants. Així, els primers (*public distributed ledger technology system*) són accessibles al públic i qualsevol hi pot participar sense que s'exigeixi el compliment de cap requisit. En canvi, els sistemes privats (*private distributed ledger technology system*) són accessibles només per a un grup limitat d'usuaris, de manera que és necessària una invitació o el compliment de certs requisits per accedir-hi. D'altra banda, els sistemes s'anomenen *permissionless* (no subjectes a permís) quan no requereixen cap autorització per realitzar una activitat concreta, qualificatiu que es refereix sense distinció tant als usuaris com als operadors del sistema, i *permissioned* (subjectes a permís) quan l'usuari o l'operador ha de comptar amb una autorització per realitzar una activitat particular. Aquestes característiques poden modular-se i combinar-se entre elles, donant lloc a múltiples variants híbrides de les TRDs.

D'altra banda, els sistemes de registre distribuït admeten tecnologies diverses, entre d'altres, les anomenades cadenes de blocs (*blockchain*), en les quals les transaccions validades s'agrupen en blocs enllaçats (o encadenats), els uns als altres, de forma cronològica, essent aquest ordre temporal el que les caracteritza enfront de la tipologia més genèrica de registre distribuït. De fet, les cadenes de blocs, que comprenen un ventall de configuracions, són el tipus més conegut de tecnologia de registre distribuït. Podem esmentar, com a exemples de xarxes públiques basades en *blockchain*, Bitcoin i Ethereum.

Sobre aquesta qüestió, seguint, novament, amb les definicions dels documents de treball del Comitè Tècnic 307 de l'ISO, una cadena de blocs és un registre distribuït amb blocs confirmats i organitzats mitjançant vincles criptogràfics en una cadena seqüencial que només permet addicions. Al seu torn, un bloc es defineix com una estructura de dades que comprèn dades de transaccions i una capçalera de bloc (enllaç criptogràfic a un bloc previ) i es confirma mitjançant l'acceptació per consens entre els diferents nodes que participen en la xarxa i guarden una rèplica dels registres sobre, d'una banda, la validesa de la transacció (relativa al compliment de les condicions exigibles d'integritat) i, d'altra, la incorporació d'un conjunt coherent i ordenat de transaccions validades. Ara bé, aquest consens, que pot diferir entre els diversos tipus de dissenys de la tecnologia, no implica necessàriament la unanimitat de tots els nodes participants, també coneguts com a «miners» (*miners*), i la seva activitat de creació i validació de registres o blocs, denominada «mineria» (*mining*).

La posada en pràctica d'aquest tipus de tecnologia emergent, tenint en compte l'heterogeneïtat del disseny de cada xarxa, els diferents mecanismes de governança i consens i les seves limitacions, planteja, a més d'oportunitats, diversos reptes sobre els quals han mostrat interès tant el sector privat com el públic, essent més abundants en el primer sector, tot i

que als nostres efectes tenen més interès les experiències en el sector públic, d'algunes dels quals farem esment seguidament.

En l'àmbit internacional, són diversos els estats que han estudiat els usos potencials de les TRDs i, entre aquestes, de les ja esmentades tecnologies de cadena de blocs, particularment en el sector públic, i que han endegat projectes basats en el seu ús.

A Europa, podem citar, a títol d'exemple, el cas d'Estònia, considerat un estat pioner en l'adopció de fórmules suportades en noves tecnologies que ofereix un ampli ventall de serveis basats en una estructura de cadena de blocs denominada *KSI Blockchain*. Aquesta tecnologia ha estat integrada, entre d'altres, en els registres públics de la propietat, mercantil i de successions i també s'utilitza en els serveis d'identificació electrònica estonians, com l'ID card (així ho afirma, per exemple, l'informe *Government services and digital identity*, d'1 d'agost de 2018, elaborat pel *Knowledge Media Institute of the Open University* per a l'Observatori i Fòrum de la Cadena de Blocs de la Unió Europea, al qual farem referència més endavant). Entre els esmentats sistemes, el govern estonià ha desenvolupat una residència digital per a estrangers (coneguda com a *e-Residency*, el llançament de la qual va tenir lloc al desembre de 2014), que permet l'accés a serveis digitals, com ara els de registre i signatura digital.

Podem fer esment, així mateix, de l'Agència Nacional de Registre Públic a Geòrgia, la qual utilitza des de l'any 2016 un sistema de cadena de blocs per inscriure els títols de propietat i validar les transaccions sobre béns immobles; el projecte desenvolupat des de 2017 per l'Autoritat Marítima Danesa (*Søfartsstyrelsen*) relatiu a la digitalització del procediment de registre de vaixells amb el suport de *blockchain*; el sistema d'identitat implementat a Finlàndia per als refugiats, vinculat a una targeta de crèdit i basat en *blockchain*, i el projecte d'identitat descentralitzada uPort impulsat

des de l'any 2017 al municipi suís de Zug, el qual permet als seus ciutadans crear una identitat fonamentada en *blockchain* independent del govern, emprada, entre d'altres, per acreditar la seva residència i votar electrònicament.

En aquest context, destaquen diverses iniciatives impulsades des de la Unió Europea, com ara els treballs de l'Observatori i Fòrum de la Cadena de Blocs de la Unió Europea, la cooperació entre els sectors públic i privat a través de la *International Association for Trusted Blockchain Applications* (INATBA) i l'*European Blockchain Partnership*, constituïda el 10 d'abril de 2018 i formada pels estats membres de la Unió Europea, Noruega i Liechtenstein amb l'objectiu d'explorar el potencial dels serveis basats en aquesta tecnologia en benefici dels ciutadans, la societat i l'economia, i d'implementar l'*European Blockchain Services Infrastructure* (EBSI), la qual proveirà serveis públics arreu del territori europeu utilitzant *blockchain*.

El 3 d'octubre de 2018 el Parlament Europeu va adoptar la Resolució sobre les tecnologies de registres distribuïts i les cadenes de blocs: fomentar la confiança amb la desintermediació. Com a punt de partida, considera que les TRDs són una constel·lació de tecnologies, amb diverses característiques tecnològiques i distints mecanismes de governança i consens (apt. 39), que estan en evolució i que necessiten un marc favorable a la innovació, que proporcioni seguretat jurídica i respecti el principi de neutralitat de la tecnologia, de manera que «todo enfoque regulatorio [...] debe ser favorable a la innovación y guiarse por los principios de neutralidad tecnológica y neutralidad del modelo empresarial, permitiendo también la creación de ecosistemas favorables a la innovación y plataformas de innovación» (considerants E i H, i apt. 65).

Dit això, emfasitza que les TRDs generen un entorn de confiança entre les parts, comporten la reducció dels costos d'intermediació i l'intercanvi de

valor entre homòlegs que pot empoderar els ciutadans, millorar els serveis i, en general, retallar les despeses en un ampli espectre de sectors fonamentals (apt. 1). Més concretament, el Parlament planteja la necessitat d'adoptar iniciatives estratègiques en diversos àmbits com l'energia i les aplicacions respectuoses amb el medi ambient, el transport, el sector sanitari, les cadenes de subministrament, l'educació, les indústries creatives i els drets d'autor i el sector financer.

Quant a la seguretat de la infraestructura, demana a la Comissió que, en el marc de l'Observatori i Fòrum de la Cadena de Blocs de la Unió Europea, observi els avenços tecnològics, avalui els riscos i doni suport a la resiliència a un ciberatac o a un col·lapse del sistema, i promogui projectes de protecció de dades que garanteixin la sostenibilitat de les plataformes de TRD (apt. 45).

Pel que ara ens ocupa, destaca també que les TRDs permeten als usuaris identificar-se i alhora controlar les dades que desitgen compartir, donant suport a l'aparició de nous models d'identitat digital que comptin amb aquest control personal sobre les dades pròpies (la denominada SSI o *self-sovereign identity*). Les identitats digitals s'estimen «imprescindibles» per al futur de la tecnologia i, en conseqüència, assenyala que els estats membres han d'intercanviar millors pràctiques sobre com garantir la seguretat de les dades. Així, insisteix en la importància que els usos de les TRDs compleixin la legislació europea sobre protecció de dades especialment en aquest àmbit i demana a la Comissió i al Supervisor Europeu de Protecció de Dades que aportin més orientacions sobre això (apt. 33). En particular, fa referència a la preocupació sobre la protecció de les dades (apts. 28, 29, 30 i 31) i les dificultats en l'aplicació de l'anomenat dret a l'oblit, és a dir, el dret de supressió de les dades personals (apt. 32).

A més, la Resolució esperona l'impuls d'iniciatives comunes per part de la Comissió i els estats membres per conscienciar i formar els ciutadans, les empreses i les administracions públiques a fi de facilitar la comprensió i l'acceptació d'aquesta tecnologia, amb l'ambició que Europa es converteixi en «el líder mundial en el àmbito de la TRD y [sigui] un actor creíble en la configuración de su desarrollo y sus mercados a nivel mundial» (apt. 77). Amb aquest fi, anima la Comissió i els estats a adoptar mesures legislatives o regulatòries en el cas que siguin necessàries, de forma harmonitzada, i remarcant que la Unió Europea «no debe regular la TRD *per se*, sino que debe intentar derribar los obstáculos a la aplicación de cadenas de bloques» (apt. 68). Això no obstant, demana a la Comissió desenvolupar un marc jurídic europeu per resoldre possibles problemes jurisdiccionals que puguin plantejar-se en cas de frau o delictes en l'intercanvi de TRD (apt. 69).

A Espanya, l'any 2016 es va crear el Consorci xarxa Alastria, una associació sense ànim de lucre, amb vocació multisectorial, promoguda per empreses, institucions i experts, que neix per accelerar la creació d'ecosistemes digitals entorn a *blockchain*, posant a disposició dels socis una plataforma col·laborativa comuna, i afavorir la implementació, l'estandardització, la protecció i l'ús de les tecnologies *blockchain* a Espanya i a escala internacional. D'acord amb la informació disponible al seu lloc web, la xarxa és pública i subjecta a permís, i està construïda sobre Quorum (basada en Ethereum), si bé no es confia el seu desenvolupament a una única plataforma i és per això que també està treballant en la creació de dues xarxes noves basades en altres plataformes com són *Parity* i *HyperLedger Fabric*. L'Associació està desenvolupant un model d'identitat digital (ID_Alustria) inspirat en el concepte *self-sovereign identity*, amb el propòsit de disposar d'una proposta per a l'estàndard europeu.

En són membres, pertanyents al sector públic, entre d'altres, el Consorci Administració Oberta de Catalunya (format per l'Administració de la

Generalitat de Catalunya i el Consorci Local per al Desenvolupament de les Xarxes de Telecomunicacions i de les Noves Tecnologies, Localret), la Junta d'Andalusia i el Govern d'Aragó, la Societat d'Informàtica del Govern Basc (*Eusko Jaurlaritzaren Informatika Elkarte*), les diputacions provincials de Lleida i Ourense, el Banc d'Espanya, la Comissió Nacional del Mercat de Valors, el Col·legi de Registradors de la Propietat, la Secretaria d'Estat d'Igualtat, la Secretaria General del Tresor i Política Financera i la Fàbrica Nacional de Moneda i Timbre-Reial Casa de la Moneda. També en formen part diverses universitats i escoles de negocis, així com el Consorci de Serveis Universitaris de Catalunya (CSUC) i la Conferència de Rectors de les Universitats Espanyoles (CRUE).

Alguns dels esmentats membres han impulsat projectes basats en tecnologia TRD, com ara la xarxa denominada Blue (Blockchain Universidades Españolas) de la CRUE, amb l'objectiu de desenvolupar i desplegar serveis en el sector acadèmic com l'emissió de certificacions. Per la seva part, el govern aragonès ha contractat un servei de presentació d'ofertes i avaluació automatitzada d'aquestes en procediments de contractació pública electrònica utilitzant una TRD.

Respecte al marc català, el 24 de juliol de 2018 el Govern de la Generalitat, en l'àmbit de l'estratègia SmartCAT aprovada el 28 d'octubre de 2014 i modificada posteriorment el 13 de desembre de 2016, va acordar impulsar la implementació de la tecnologia *blockchain* a l'activitat de les administracions públiques catalanes amb els objectius de posicionar Catalunya com a capdavantera en l'ús i en el desenvolupament d'aquesta tecnologia; impulsar l'ús, per part de l'Administració pública, de la tecnologia *blockchain* per oferir millors serveis i amb més transparència, i promoure, entre la ciutadania, les possibilitats i potencialitats d'aquesta tecnologia per facilitar-ne l'adopció i la seva participació, entre d'altres (Acord GOV/65/2018, de 24 de juliol). Gairebé un any després, el 18 de juny de 2019, el Govern va aprovar

l'Estratègia *blockchain* de Catalunya, que preveu el desplegament d'un programa d'actuacions al voltant de sis eixos, entre els quals podem destacar: en l'Administració pública, amb l'objectiu de millorar els serveis públics mitjançant l'adopció de les tecnologies *blockchain* i TRD, i en la regulació, per tal d'analitzar les implicacions que aquesta té sobre el desplegament de l'esmentada tecnologia i també com es regulen les aplicacions que en fan ús. L'Estratègia descriu, entre les possibles aplicacions que poden desenvolupar-se, la identitat digital dels usuaris.

Recentment, el Govern ha fet públic el projecte IdentiCAT, definit, segons la informació divulgativa disponible al lloc web del Departament de Polítiques Digitals i Administració Pública, com un nou model d'identitat digital basada en TRD i desenvolupada amb l'objectiu de millorar les mesures de seguretat i privacitat en els sistemes d'identificació digital. De fet, el Parlament de Catalunya, en la sessió del dia 26 de setembre de 2019, va instar el Govern de la Generalitat a «[i]mpulsar el projecte IdentiCAT com a eina d'apoderament de la ciutadania en l'entorn digital, per tal que siguin els mateixos ciutadans els que tinguin el control i el govern de llurs dades personals en qualsevol relació digital» (Resolució 546/XII del Parlament de Catalunya, sobre l'orientació política general del Govern, publicada al BOPC núm. 431, de 4 d'octubre de 2019).

D'acord amb la informació publicada al lloc web esmentat, s'afirma que amb l'IdentiCAT s'instaura un sistema d'identitat autosobirana i descentralitzada en el sentit que és el ciutadà mateix qui «té el control total de les seves dades» mentre que, fins ara, aquestes les «custodiava l'entitat/organisme emissor i validador de la identitat», de manera que desapareix l'autoritat de certificació i la Generalitat de Catalunya adopta el paper de «validador segur [...] proporcionant eines i un marc fiable, legal i adaptatiu per a la ciutadania i les empreses públiques i privades». Entre altres i nombroses opcions, el

projecte es podria dissenyar com una xarxa pública de TRD no subjecta a permís (*permissionless*).

3. L'enquadrament competencial, que vàrem exposar en el fonament jurídic 3.2.B del DCGE 6/2019 sobre l'article 3 RDL 14/2019, ens és d'utilitat també per a l'apartat tres d'aquest precepte, que afegeix una nova disposició addicional sisena a la LPACAP que regula la mateixa submatèria, relativa als sistemes d'identificació i de signatura electròniques dels interessats davant de les administracions públiques. A mode de recordatori, resumirem el que hi vàrem dir, tot aplicant-ho a l'article 3.tres RDL 14/2019, per tal de delimitar quin és el seu règim competencial.

Començarem invocant la disposició final primera RDL 14/2019, que enuncia els títols competencials que avalen la seva regulació. En el seu apartat 2, quan hi fa referència a l'article 3 (i 4) RDL 14/2019, diu que aquest es dicta a l'empara de les clàusules competencials 18 (bases del règim jurídic de les administracions públiques i el procediment administratiu comú) i 29 (seguretat pública) de l'article 149.1 CE. La invocació indistinta dels dos títols de l'Estat ens porta a la necessitat de determinar quin és el d'aplicació prevalent a fi de resoldre la controvèrsia competencial plantejada a la petició de dictamen dels grups parlamentaris.

Concretament, d'una banda, pel que fa a l'apartat primer de la nova disposició addicional sisena LPACAP, el preàmbul del Reial decret llei (apt. II, par. 9è) indica que es dicta en exercici de la competència estatal per establir la legislació bàsica; per tant, d'acord amb la disposició final primera.2 RDL 14/2019 suara exposada, no pot ser altra que la prevista a l'article 149.1.18 CE, sense que l'esmentada disposició addicional sisena.1 en digui res més. D'altra banda, quant a l'apartat segon, el seu text conté una referència explícita a la seguretat pública, com també s'hi refereix el preàmbul (apt. II, par. 8è i 9è), cosa que ens remet a l'article 149.1.29 CE.

Respecte de l'anterior, en el Dictamen 6/2019 vàrem enquadrar prevalentment la regulació de l'article 3 RDL 14/2019 en les bases del règim jurídic de les administracions públiques i el procediment administratiu comú, ja que l'aspecte de seguretat principalment afectat pel contingut i la finalitat del precepte era el de la seguretat de les xarxes i comunicacions electròniques de les distintes administracions, descartant la seguretat pública *stricto sensu*, que és un títol competencial diferent.

Així, com dèiem al fonament jurídic 3.1.B del reiterat Dictamen, la competència en seguretat pública ha estat precisada pel Tribunal Constitucional en diverses sentències. A tall de síntesi, aquest ha declarat que se n'ha de fer una interpretació restrictiva, de manera que es tracta «de un concepto más estricto en el que hay que situar de modo predominante las organizaciones y los medios instrumentales, en especial los cuerpos de seguridad». Per tant, no tota seguretat de persones i béns, ni tota normativa encaminada a assolir-la o a preservar el seu manteniment poden incloure's en aquesta matèria (STC 25/2004, de 26 de febrer, FJ 6). La seguretat pública s'ha d'acotar, doncs, d'acord amb el context on se cita, atès que pot remetre a continguts tan diferents com la «seguretat nacional», la seguretat pública en sentit estricte o la seguretat de les xarxes digitals.

Segons això, a l'entorn digital de les administracions públiques li escau més la denominada ciberseguretat circumscrita a l'Administració electrònica (definida al DCGE 5/2017, de 29 de juny, FJ 2.1), que s'encabeix en el marc competencial delimitat pels articles 149.1.18 CE i 159 EAC, que admet la potestat legislativa de la Generalitat dins de les bases estatals sobre la seguretat de les seves xarxes i en les relacions amb els administrats, tant en el sentit de la seva fiabilitat, com en el de ciberseguretat.

4. En el fonament jurídic 3.2.C de l'esmentat DCGE 6/2019, relatiu a l'article 3 RDL 14/2019, hem entès, doncs, que la regulació dels sistemes autoritzats d'identificació i de signatura electròniques dels interessats davant de les administracions públiques s'inscriu en l'abans esmentat marc competencial de caràcter compartit entre l'Estat i les comunitats autònomes (art. 149.1.18 CE i 159 EAC), analitzat en el precitat Dictamen.

A tall de recordatori, quant al règim jurídic de les administracions públiques, hem afirmat que aquest títol competencial permet «establecer los elementos esenciales que garantizan un régimen jurídico unitario aplicable a todas las Administraciones públicas» (STC 50/1999, de 6 d'abril, FJ 3), és a dir, «los principios y reglas básicos sobre los aspectos organizativos y de funcionamiento de todas las Administraciones públicas, garantizando un régimen jurídico unitario para todas ellas (SSTC 32/1981, de 28 de julio, FJ 5, y 227/1988, de 29 de noviembre, FJ 24)» (STC 132/2018, de 13 de desembre, FJ 4). La intensitat d'aquestes normes bàsiques s'accentuarà quan es tracti d'aspectes que afecten directament l'activitat externa de l'Administració, especialment en la seva relació amb els administrats (STC 50/1999, FJ 3, i DCGE 5/2017, FJ 2.3 i 3.5).

Amb caràcter més general, segons la jurisprudència constitucional, les bases han d'establir el mínim comú denominador normatiu, assegurant un marc normatiu unitari, d'aplicació a tot el territori espanyol (STC 197/1996, de 28 de novembre, FJ 5.A, i 235/1999, de 20 de desembre, FJ 15). Ordinàriament han de ser principis o directrius que permetin un desenvolupament legislatiu, de forma que no arribin a un nivell de detall o completesa que pràcticament impedeixi l'adopció de polítiques pròpies autonòmiques (STC 50/1999, FJ 3, i 130/2013, de 4 de juny, FJ 6), com diu també l'article 111 EAC, en relació amb la Generalitat.

Les bases, però, poden tenir una intensitat i un abast variables en funció del subsector material sobre el qual es projecten (STC 18/2011, de 3 de març, FJ 9). Així, en la STC 165/2016, de 6 d'octubre, se citen algunes modalitats de bases, confirmant que no es tracta d'una tècnica normativa uniforme, sinó que s'adapta a les característiques de la qüestió concretament afectada. Literalment, la resolució exposa diferents abast i tipologies de les bases estatals:

«desde la posibilidad de que el legislador estatal, excepcionalmente ocupe, prácticamente, toda la función normativa al determinar las bases de determinadas submaterias, hasta la legitimidad constitucional de algunos actos administrativos de carácter eminentemente ejecutivo por parte de la Administración General del Estado, así como el empleo de otras modalidades muy diversas (topes máximos, niveles mínimos, tramos, e, incluso, bases diferenciadas por territorios, etc.).» (FJ 11)

Ara bé, si l'Estat no dicta les normes bàsiques en un determinat àmbit on té constitucionalment reconeguda aquesta intervenció competencial, això no hauria d'impedir que les comunitats autònomes despleguin la seva regulació en aquell àmbit, inferint allò que són bases de l'ordenament jurídic, en exercici de les competències estatutàriament assumides (entre d'altres, STC 32/1981, de 28 de juliol, FJ 6; 64/1982, de 4 de novembre, FJ 5; 48/1988, de 22 de març, FJ 3; 197/1996, de 28 de novembre, FJ 5; 101/2005, de 20 d'abril, FJ 5; 135/2012, de 19 de juny, FJ 4, així com DCC núm. 204, de 20 de gener de 1998, F III, i DCGE 1/2017, de 26 de gener, FJ 3.4).

En el cas que posteriorment es dicti legítimament una legislació bàsica específica sobre els sistemes d'identificació i de signatura electròniques dels interessats davant les administracions públiques que sigui incompatible amb l'autonòmica, aquesta, que originàriament i eventual era respectuosa amb

l'ordre constitucional de distribució de competències, ha de ser acomodada a les bases estatals (STC 204/2016, d'1 de desembre, FJ 3).

Pel que ara interessa i com vàrem indicar en el DCGE 6/2019 (FJ 3.2.D), els articles 9 i 10 LPACAP contenen un seguit de previsions bàsiques dictades per l'Estat a l'empara de les seves competències sobre règim jurídic de les administracions públiques i procediment administratiu comú (art. 149.1.18 CE). Singularment, segons l'actual versió arran de la reforma operada pel Reial decret llei, es prescriu l'acceptació dels sistemes d'identificació i de signatura electròniques garantits i que proporcionen majors nivells de seguretat, que són els previstos en les lletres *a* i *b* dels articles 9.2 i 10.2 LPACAP. Com a conseqüència de l'anterior, les administracions públiques han d'assegurar que els administrats puguin utilitzar qualssevol d'aquests sistemes en tots els procediments i en tots els seus tràmits (art. 9.2.c 2n par. i 10.2.c 2n par. LPACAP). Així mateix, pel que fa als sistemes d'identificació electrònica, les administracions han d'admetre l'acreditació dels interessats en el procediment administratiu mitjançant els sistemes acceptats per l'Administració general de l'Estat (incloent-hi els d'altres estats membres que l'Estat hagi reconegut), llevat que hi hagi una prova en contra (art. 9.4 LPACAP). Per tant, només si el sistema no és idoni per al concret tràmit o servei, l'administració afectada podrà oposar-se a la seva utilització. I les administracions públiques poden admetre els sistemes d'identificació com a sistemes de signatura quan així ho disposi la normativa reguladora aplicable i sempre que permetin acreditar l'autenticitat de l'expressió de la voluntat i el consentiment dels interessats (art. 10.4 LPACAP).

A banda dels límits anteriors, es reconeix a les administracions públiques la competència per dissenyar els seus propis sistemes d'identificació i de signatura electròniques, segons les seves necessitats i les característiques de l'actuació administrativa corresponent. Per tant, poden optar per la implementació d'altres sistemes més senzills que considerin vàlids (p. ex. de

clau concertada), en els termes i les condicions que s'estableixin, sempre que comptin amb un registre previ com a usuari que permeti assegurar la seva identitat (art. 9.2.c 1r par. i 10.2.c 1r par. LPACAP). En aquest punt, cal que ens remetem al que vàrem dir en el DCGE 6/2019, en el sentit que hem considerat inconstitucional i antiestatutària perquè vulnera el marc competencial dels articles 149.1.18 CE i 159 EAC la previsió que l'Estat hagi d'autoritzar amb caràcter previ l'adopció d'aquests sistemes per part de les administracions públiques, que ha estat introduïda pel Reial decret llei 14/2019 en la nova redacció dels articles 9.2.c i 10.2.c LPACAP, com hem recordat en el fonament jurídic precedent d'aquest Dictamen.

Finalment, s'estableix l'obligació de localitzar els recursos tècnics necessaris per gestionar els dits sistemes en territori de la Unió Europea (art. 9.3 i 10.3 LPACAP).

En aquest mateix àmbit, la regulació del Reglament (UE) núm. 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i per la qual es deroga la Directiva 1999/93/CE (en endavant, Reglament eIDAS), al qual ens hem referit a bastament en el DCGE 6/2019, fixa uns continguts comuns per a tota la Unió Europea, que constitueixen un marc regulatori general que és de directa i obligatòria observança per a tots els estats membres. Així, entre d'altres, els principis i les prescripcions com ara el de la neutralitat tecnològica (considerants 16 i 27, art. 12.3.a Reglament eIDAS), el reconeixement mutu o recíproc (considerants 6, 10, 11, 14, 19, 20 i 48 i art. 6 Reglament eIDAS) i la categorització dels diferents nivells i requisits de seguretat de la identificació electrònica, entre d'altres (art. 8 i 26, Reglament eIDAS, i Reglament d'execució 2015/1502 de la Comissió, de 8 de setembre de 2015), són aplicables als sistemes previstos en les lletres *a* i *b* dels articles 9.2 i 10.2 LPACAP, però també ho serien als sistemes a què es refereixen les

lletres c, per al cas que les administracions públiques, en funció del seu major o menor interès, optessin perquè els seus instruments d'identificació i de signatura electròniques fossin interoperables i reconeguts en un context transfronterer (considerant 15 i art. 6.2 Reglament eIDAS).

Ultra això, sobre les mesures de seguretat en aquest entorn, tal com vam apuntar en el DCGE 6/2019, el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica, dictat a l'empara de la competència estatal ex article 149.1.18 CE, defineix, entre d'altres, les que amb caràcter de mínims han d'aplicar les administracions públiques en relació amb la identificació, l'autenticació i la firma electròniques, les quals poden ser ampliades segons les circumstàncies del cas concret.

Quant a la identificació, disposa que es realitzi d'acord amb els mecanismes previstos a la legislació europea i nacional en la matèria, i determina la correspondència entre els nivells de la dimensió d'autenticitat dels sistemes d'informació als quals s'accedeix i els nivells de seguretat (baix, substancial o alt) dels sistemes d'identificació electrònica previstos al Reglament eIDAS (epígraf 4.2.1 de l'annex II). Pel que fa a la signatura electrònica, recull les mesures de protecció aplicables segons els nivells de seguretat requerits pel sistema i precisa que si s'utilitzen altres mecanismes de signatura electrònica subjectes a dret s'han d'incorporar mesures compensatòries suficients que ofereixin garanties equivalents o superiors en allò relatiu a la prevenció de la repudiació, d'acord amb l'article 27.5 del Reial decret 3/2010 (epígraf 5.7.4 del mateix annex).

Fetes les consideracions anteriors, és evident que el vigent ordenament jurídic conté un conjunt de bases estatals que garanteixen la seguretat dels sistemes d'identificació i de signatura electròniques dels interessats en les seves relacions amb les administracions públiques, que són aplicables a les

noves tecnologies que es desenvolupin. Altrament, també ho són, com hem vist, les previsions relatives a la seguretat del Reglament eIDAS, a banda del respecte a la regulació europea i espanyola de protecció de dades personals.

5. A continuació, analitzarem els dos apartats de la disposició addicional sisena LPACAP, als quals aplicarem el cànon de constitucionalitat i d'estatutarietat fins ara descrit.

En particular, l'apartat primer de la disposició addicional sisena LPACAP (art. 3.tres RDL 14/2019) exceptua l'aplicació del que disposa l'apartat c dels articles 9.2 i 10.2 LPACAP (art. 3.u i .dos RDL 14/2019) a determinats sistemes d'identificació i de signatura electròniques dels interessats davant de les administracions públiques susceptibles de ser validats per aquestes, si no es compleix ulteriorment una assenyalada condició. En concret, el precepte qüestionat per la sol·licitud prescriu, en termes absoluts, que «no són admissibles en cap cas, i per tant no es poden autoritzar» els dits sistemes d'identificació i de signatura quan es basin en tecnologies de registre distribuït.

Aquest veto és vigent mentre l'esmentada tipologia de sistemes no sigui objecte d'una regulació específica per part de l'Estat en el marc del dret de la Unió Europea. El preàmbul del Reial decret llei considera que «[l]es restriccions imposades [...] en cap cas no suposen una prohibició general. Simplement, se'n restringeix puntualment i d'una manera merament provisional l'ús com a sistema d'identificació i signatura dels interessats» davant les administracions públiques. Això ho justifica perquè, al seu parer, de moment no hi ha prou coneixement ni «un marc regulador *ad hoc* de caràcter estatal o europeu que faci front a les debilitats que implica el seu ús per a les dades i la seguretat pública» (apt. II, par. 9è).

D'acord amb l'article 149.1.18 CE, l'Estat pot establir bases en l'àmbit descrit (la disciplina sobre la identificació i signatura electròniques dels interessats en les seves relacions amb les administracions públiques) sempre que preservin els marges d'autoorganització de les administracions públiques autonòmiques i les seves competències en aquesta matèria. Això és, que aquestes administracions han de poder adoptar les decisions relatives al model d'organització i funcionament de la seva administració electrònica i de les relacions digitals que mantenen amb els ciutadans i, en concret, dels sistemes d'identificació i de signatura electròniques i de la tecnologia en la qual es basaran que considerin que s'ajusta més a les seves necessitats.

Així ho ha reconegut expressament el Tribunal Constitucional, quan ha declarat que les polítiques autonòmiques en l'àmbit de la identificació electrònica (art. 9 LPACAP, versió anterior a la reforma pel RDL 14/2019) poden ser molt diverses. Per tant, les comunitats autònomes poden optar per emprar sistemes que puguin tenir virtualitat en altres estats membres de la Unió Europea, o bé poden ser proclius a utilitzar instruments senzills de baix nivell de seguretat per a ús domèstic. De fet, va considerar el precepte examinat respectuós amb el marc competencial dels articles 149.1.18 i 159 EAC perquè garantia el tractament comú dels administrats mitjançant l'atribució als ciutadans del dret a utilitzar davant de qualsevol administració pública els sistemes d'identificació electrònica que hagin estat admesos per l'Administració general de l'Estat, al mateix temps que preservava amplis marges d'autoorganització de les administracions públiques en aquest entorn (STC 55/2018, de 24 de maig, FJ 9).

Amb tot, la regulació governamental pretesament bàsica que és objecte del Dictamen, com veurem, no respecta aquesta darrera observació de caràcter competencial. Es tracta d'una mesura de naturalesa singular que proscriu de manera preventiva l'ús d'una determinada tecnologia per part de les administracions públiques, tot posposant la seva futura admissió a l'eventual

compliment d'una condició indefinida en el temps, la realització de la qual depèn, de fet, de l'Estat mateix. I adopta aquesta solució tan expeditiva en comptes d'establir, com li pertocaria competencialment, els principis o criteris que les administracions públiques haurien de respectar, en relació amb aquesta tecnologia, i que constituïrien unes bases més estandarditzades, a l'empara de la matèria reservada a l'Estat per l'article 149.1.18 CE.

En efecte, l'article 3.tres RDL 14/2019 prohibeix que les administracions autonòmiques facin ús d'una concreta tecnologia a l'hora de dissenyar i implementar els seus propis instruments administratius d'identificació i de signatura electròniques i ho fa, a més, sense donar cap orientació, que podria ser de caràcter bàsic. Ultra això posposa indefinidament l'exercici d'aquesta competència autonòmica a una regulació, de moment inexistente, que, segons la dicció de la disposició addicional sisena.1 RDL 14/2019, correspon dictar a l'Estat mateix.

A més, s'aparta, com veurem, de la voluntat neutral i més aperturista del Reglament eIDAS (considerants 16 i 26) i de les resolucions aprovades pel Parlament Europeu en aquest sector. Altrament, tampoc no s'albira què succeiria si, en aplicació d'aquella norma europea i el seu principi de reconeixement mutu (art. 6), l'Estat espanyol admet la validesa de sistemes d'identificació i de signatura electròniques d'altres estats membres basats, precisament, en la tecnologia de registre distribuït. Aquest seria el cas de diversos sistemes estonians d'identitat electrònica notificats a la Comissió Europea d'acord amb l'article 9.1 del Reglament eIDAS per tal que siguin reconeguts per part de la resta d'estats membres, com ara l'*e-Residency* i l'*ID card*, entre d'altres (DOUE C núm. 401, de 7 de novembre de 2018). Sobre la tecnologia emprada per aquests sistemes, ens remetem a les referències realitzades en l'apartat B anterior.

La possibilitat de dictar normes bàsiques estatals de caràcter prohibitiu, que permeten un estret marge de desenvolupament autonòmic, ha estat acceptada en alguns supòsits per la jurisprudència constitucional, tenint en compte la matèria en la qual s'emeten (especialment en l'àmbit estrictament econòmic o de finalitats ambientals).

En un pronunciament en relació amb l'article 149.1.18 CE, el Tribunal Constitucional, a partir d'una qüestió d'inconstitucionalitat, ha considerat bàsiques les excepcions a la prohibició de regular el pagament ajornat del preu dels contractes administratius d'obra. La STC 56/2014, de 10 d'abril, diu que l'esmentat precepte constitucional atribueix a l'Estat la competència per dictar la legislació bàsica sobre contractes i concessions administratives (FJ 3), la qual té un abast i una naturalesa diferents de les altres competències recollides en la mateixa regla competencial (STC 61/1997, de 20 de març, FJ 11). Igualment, afirma que la prohibició establerta ho ha estat perquè tradicionalment és una regla general en dret espanyol, a fi de contenir el creixement de la despesa pública i el nivell d'endeutament i assegurar el manteniment de l'equilibri pressupostari, cosa que està en connexió amb l'objectiu d'estabilitat pressupostària, constitucionalitzat en l'article 135 CE, i que es configura com una orientació de la política econòmica general que l'Estat pot dictar ex article 149.1.13 CE (STC 56/2014, FJ 4). La decisió jurisprudencial també en aquest cas es vincula a les competències econòmiques reservades a l'Estat, tot i que es pronuncia estrictament en relació amb l'article 149.1.18 CE.

Ara bé, les bases prohibitives també han estat rebutjades en altres ocasions, quan no permeten el desenvolupament de les competències autonòmiques en una matèria compartida. La STC 68/2017, de 25 de maig, va confirmar la posició d'aquest Consell en el DCGE 26/2015, de 29 de desembre, en l'àmbit de l'autoconsum elèctric, en el que vàrem considerar contrària a les competències de la Generalitat una determinada prohibició («en cap cas un

generador es pot connectar a la xarxa interior de diversos consumidors»). Al respecte, varem afirmar que «no trobem al preàmbul ni tampoc a la documentació complementària de què disposem cap dada que justifiqui les raons d'aquesta prohibició, que no sembla que sigui la més adequada per fer efectives les previsions de futur a què es refereix la Directiva». Es tractava d'una prohibició que no permetia a la Generalitat el desenvolupament de l'exercici de la seva competència compartida en matèria energètica. Per això, consideràvem que:

«En tot cas, a parer nostre, aquesta norma no pot gaudir de la consideració de bàsica, que, com hem dit, tampoc es dedueix del preàmbul ni de la mateixa redacció del precepte. En aquest sentit, el Govern de l'Estat hauria pogut establir algunes cauteles respecte d'aquest tema, determinant límits en funció de les característiques de la xarxa de distribució en zones determinades, i també amb la finalitat de protegir-ne la sostenibilitat tècnica i econòmica.

Aquests límits o aquestes cauteles podrien adequar-se a la naturalesa de la norma bàsica, sempre que permetessin el seu desenvolupament legislatiu i reglamentari per part de les comunitats autònomes, d'acord amb les característiques de la seva xarxa de distribució o, fins i tot, amb la finalitat d'establir polítiques pròpies en la matèria.» (FJ 3.2)

A la Sentència abans citada, el Tribunal Constitucional va corroborar que la prohibició esmentada «carece de naturaleza básica», de forma que incorre en extralimitació competencial i és inconstitucional i nul·la (STC 68/2017, FJ 6).

Aquesta doctrina s'ha d'aplicar al cas que estem analitzant, amb més motiu pel fet que no es tracta d'una prohibició en el sentit de mera limitació que ha d'observar la Generalitat a l'hora de regular i executar una matèria, com era el supòsit referit a la STC 56/2014, abans citada, i a d'altres similars. Al contrari, més enllà del que seria una base pròpiament dita, mitjançant la prohibició d'una específica tecnologia, deixa sense efecte l'exercici d'una

competència que correspon a les comunitats autònomes. Certament, si el legislador estatal disposa que la utilització de qualssevilla de les noves tecnologies no és admissible, està desnaturalitzant i pràcticament impedit la possibilitat d'establir una política pròpia en el sector afectat. I això és així perquè, per definició, adoptar una política concreta en un determinat entorn comporta la capacitat de la Generalitat de triar lliurement entre les diverses possibilitats, en funció de les que li resultin més adequades o idònies segons les seves necessitats. En aquest cas, respecte al disseny i la configuració pròpia dels instruments administratius d'identificació i de signatura electròniques en les relacions digitals dels ciutadans amb l'Administració pública catalana.

En aquest sentit, el mateix legislador estatal reconeix que correspon a les comunitats autònomes aquesta competència, l'exercici de la qual pot desplegar la Generalitat des de l'aprovació de la LPACAP, alhora que li ha estat reconeguda per la doctrina constitucional i consultiva (STC 55/2018, FJ 9, i DCGE 23/2015, de 17 de desembre, FJ 3.1.B). Però, a continuació, amb la incorporació de la disposició addicional sisena pel Reial decret llei, afegeix una prohibició que la interromp de manera indefinida, deixant, a més, a la voluntat de l'Estat el moment en què pot recuperar-la.

Vist l'anterior, es tracta d'una previsió si més no peculiar que, pel seu caràcter fortament restrictiu, merita una explicació fonamentada i raonada que en justifiqui l'adopció, ateses les seves característiques. En altres paraules, si s'estableix una prohibició d'aquesta índole, excepcional per la seva naturalesa mateixa, pel cap baix s'hauria de justificar i motivar, en l'articulat o en l'exposició de motius de la norma objecte de dictamen. No oblidem que l'Estat s'arroga una potestat de la Generalitat (com és el disseny dels sistemes d'identificació i de signatura dels interessats en les seves relacions amb l'Administració catalana) que troba empara en l'article 159 EAC.

En conseqüència, haurem de verificar si, en el Reial decret llei, més enllà de la referència recurrent a la seguretat pública, hi ha alguna motivació que justifiqui una mesura com la prevista en el seu article 3.tres. En la nova disposició addicional sisena.1 LPACAP no hi ha cap justificació de la regla prohibitiva que s'hi conté, per la qual cosa haurem d'examinar si en el preàmbul hi trobem una fonamentació racional i suficient que justifiqui la seva adopció.

En el proemi de la disposició legislativa del Govern, com hem vist, hi ha una argumentació genèrica que invoca la manca de dades o de coneixement sobre la tecnologia vetada i manté la prohibició «mentre no hi hagi més dades o un marc regulador *ad hoc* de caràcter estatal o europeu que faci front a les debilitats que implica el seu ús per a les dades i la seguretat pública».

En relació amb la manca de coneixement esmentada, abans de prohibir de forma absoluta una tecnologia, que, segons el que es desprèn de la citada Resolució europea, no és negativa en si mateixa i té avantatges, es pot testar de forma parcial. De fet, la dita tecnologia, que s'anuncia com un progrés innegable, ha tingut aplicació en l'àmbit privat, especialment en el món de les criptomonedes, ja fa més de deu anys. Certament, la seva aplicació en el sector públic és relativament incipient i planteja reptes jurídics per resoldre, per la qual cosa una regulació cautelosa és necessària, però també es constata que s'hi ha anat incorporant progressivament amb diverses aplicacions tecnològiques, com hem vist al principi d'aquest fonament jurídic.

A tall il·lustratiu, cal recordar que en el DCGE 9/2017, de 24 d'agost, sobre el Projecte de llei del procediment de votació electrònica per als catalans residents a l'estranger vàrem constatar l'escassa aplicació que tenia la

varietat de sistemes de vot per internet, però al mateix temps vàrem posar en relleu l'avenç considerable que representava per a la participació dels ciutadans en els processos electorals i la decidida aposta europea pel vot electrònic (FJ 2), tot i que vàrem recordar que:

«encara que no ens pertoca pronunciar-nos sobre aspectes tècnics relatius als programes i els mitjans que seran utilitzats per a l'aplicació del vot per internet, [...] sí que considerem necessària, com una mesura mínima de prudència, la realització de proves i de tests previs que demostrin la qualitat dels sistemes electrònics i la seva aptitud per evitar els riscos que poden afectar tot sistema de vot per internet. Ens referim a proves experimentals o pilot, fins i tot en la línia dels denominats tests d'estrès i de simulació d'amenaces, i també a assajos sobre el funcionament real del sistema en el procés electoral, encara que sense efectes vinculants per a la validesa del vot.» (FJ 3)

Amb una prevenció semblant, el Parlament Europeu demana a la Comissió Europea que col·labori amb els estats membres per posar en marxa i supervisar casos d'ús i projectes pilot que utilitzin la *blockchain* en l'entorn dels serveis públics i perquè les autoritats competents i la Comissió desenvolupin proves de resistència (Resolució de 3 d'octubre de 2018, apts. 46, 48, 54, 68, 70 i 75).

En aquest sentit, és evident que són imaginables altres fórmules que permetin equilibrar el principi de precaució i el d'innovació i que serien molt més respectuoses i menys lesives amb la competència d'autoorganització de les administracions públiques que no pas optar per la prohibició, sense més ni més, d'una tecnologia —que té una varietat molt àmplia d'aplicacions— per donar suport als instruments administratius propis. A tall d'exemple, es podria establir un *sandbox* per analitzar el desenvolupament del sistema d'identificació i de signatura electròniques mitjançant TRD, el qual constitueix un entorn segur que permet realitzar proves i facilitar el procés de

transformació digital dels poders públics. Així es va preveure en el cas de l'avantprojecte de mesures per a la transformació digital del sector financer, que dedicava el seu títol II a regular un espai controlat de proves, precisament per emparar que es duguessin a terme projectes pilot a mode de proves experimentals, de manera controlada i delimitada (art. 3 a 23).

Com se sap, l'autonomia política pressuposa legislar i establir noves formes d'organització, que tindran consolidacions diverses, però dins de les competències inclou la capacitat de desenvolupar polítiques pròpies, que fructifiquin o no. L'Estat, en virtut de la seva competència, prevista a l'article 149.1.18 CE, pot establir bases que donin unes orientacions comunes a fi de garantir un model homogeni de sistema jurídic regulador de les administracions públiques, que permeti disposar als administrats d'un tractament comú davant de les administracions (STC 50/1999, FJ 3). En concret, quant als sistemes d'identificació i de signatura electròniques, ja hem vist que garanteix aquest tractament comú, entre d'altres, quan imposa l'acceptació per part de totes les administracions dels sistemes que considera que tenen major nivell de seguretat o confiança (art. 9.2.a, .b i .c, segon paràgraf, i art. 10.2.a, .b i .c, segon paràgraf, LPACAP) (STC 55/2018, FJ 9) i, a més, ha aprovat també un conjunt de previsions bàsiques en matèria de seguretat (l'esmentat Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica).

Seguint amb el preàmbul del Reial decret llei, aquest es refereix a «les debilitats que implica el seu ús [la tecnologia de registre distribuït] per a les dades i la seguretat pública». Entenem que, amb la referència a «les dades», vol advertir que la protecció de dades personals no està prou garantida i que «la seguretat pública» s'empra una vegada més en el sentit de seguretat de les xarxes, qüestions aquestes que haurien de ser tractades en «un marc regulador *ad hoc* de caràcter estatal o europeu» (apt. II par. 9è). L'exposició

de motius es limita a enunciar uns temes, sense explicar en què consisteix el seu caràcter problemàtic, ni com el Reial decret llei hi posa solució.

No és fàcil determinar l'abast exacte d'aquestes consideracions, encara que podem suposar que la crítica referència a les «debilitats que implica el seu ús per a les dades» es pot relacionar amb les qüestions i inquietuds que es planteja la Resolució del Parlament Europeu, abans comentada, que insta al compliment de la normativa europea sobre protecció de dades en l'ús de les tecnologies de registre distribuït.

Certament, la utilització poc curosa de les TRDs podria presentar problemes en aquestes i altres qüestions. Així, a títol indicatiu i en l'àmbit de la seva tasca d'anàlisi i d'informe, l'Observatori i Fòrum de la Cadena de Blocs de la Unió Europea ha publicat l'Informe de 27 de setembre de 2019, amb el títol *Legal and regulatory framework of blockchains and smart contracts*, que es refereix, entre d'altres, als problemes de territorialitat i anonimat que dificulten la determinació de la legislació aplicable i la jurisdicció competent per a la solució dels conflictes que puguin sorgir.

Per la seva part, l'Informe de l'estudi publicat pel Servei de Recerca Científica del Parlament Europeu sobre cadena de blocs i el Reglament general de protecció de dades, mitjançant un informe publicat al juliol de 2019 i adreçat als membres i el personal del Parlament Europeu per facilitar l'exercici de les seves tasques, concreta a la seva conclusió les «tensions» existents entre la tecnologia de cadena de blocs i el 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 les dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades; en endavant, RGPD) en dos aspectes substancials:

D'una banda, el RGPD es basa en el supòsit subjacent que a cada punt de dades personals hi ha almenys una persona física o jurídica, el responsable de dades, a qui poden dirigir-se els interessats per exercir els drets reconeguts per la legislació europea. En canvi, diu, la cadena de blocs sovint substitueix aquest actor unitari per molts nodes diferents, la qual cosa dificulta l'assignació de les responsabilitats que podrien derivar-se'n, especialment atesos els contorns incerts de la noció de corresponsabilitat del tractament emprada en el Reglament europeu.

I, de l'altra, el RGPD es basa en el supòsit que les dades poden rectificar-se o cancel·lar-se quan sigui necessari per complir les exigències legals com ara les previstes als articles 16 i 17 RGPD, relatius als drets de rectificació i supressió de les dades personals. En canvi, els sistemes de cadenes de blocs dificulten aquests canvis, amb la finalitat de garantir la integritat de les dades i la màxima confiança en la xarxa.

Això no obstant, en la conclusió final també destaca que *blockchain* pot oferir avantatges des de la perspectiva de la protecció de dades personals si es dissenya específicament per complir amb aquesta finalitat.

Ara bé, ambdós informes adverteixen que pot resultar més difícil superar aquests inconvenients quan es tracti de cadenes de blocs configurades com a públiques i no subjectes a permís (*permissionless*). És més, tenint en compte que, com hem vist, hi ha molts tipus diferents de *blockchain*, la seva compatibilitat amb el RGPD només pot avaluar-se cas per cas (segons la conclusió de l'Informe publicat pel servei de recerca del Parlament Europeu).

Un cop exposats els documents d'investigació i anàlisi anteriors, hem de resoldre si les «debilitats» de les TRDs al·legades al preàmbul del Reial decret llei que dictaminem justifiquen la prohibició continguda a la nova

disposició addicional sisena LPACAP. I ho farem partint de tres consideracions prèvies, que desenvoluparem seguidament.

En primer lloc, estem tractant únicament de l'aplicació de les TRDs als sistemes d'identificació i de signatura electròniques dels interessats davant les administracions públiques, en els quals moltes de les qüestions abans indicades (com ara la territorialitat i l'anonimat) serien esmenables segons la configuració concreta que adoptessin. D'aquesta manera, en allò referit a la protecció de dades, es pot fer esment també d'un altre Informe de l'Observatori europeu, de 16 d'octubre de 2018, de títol *Blockchain and the GDPR* que recorda que per a les *blockchain* privades i amb permís (*permissioned*), operades, entre d'altres, per agències governamentals serà més fàcil, ateses les característiques d'aquesta tipologia de cadena, complir amb les previsions del RGPD. Així, afegeix que les autoritats públiques que, si escau, les gestionin estan en condicions de definir les funcions dels participants i d'imposar regles estrictes per al tractament de les dades.

En segon lloc, aquestes debilitats no semblen justificar la prohibició d'una concreta tecnologia per part de l'Estat. Si es volen limitar els possibles problemes jurídics que poden ocasionar determinades TRDs, el que pot fer aquest és establir cauteles i normes de mínims, que després podran ser desenvolupades pel legislador autonòmic. Per exemple, limitant l'ús de les aplicacions de les TRDs que presentin més dificultats, o establint estàndards mínims de seguretat per a la seva aplicació. Com llegim en el darrer informe citat de l'Observatori europeu, hi ha fórmules per fer compatibles les cadenes de blocs amb el RGPD, ja que el compliment d'aquest Reglament no és qüestió de la tecnologia, sinó de com és utilitzada.

Finalment, no podem oblidar que les TRDs ofereixen avantatges importants per a la posada en marxa de projectes de governança política, àmpliament tractats a un estudi europeu de recerca i assessorament a la Comissió

Europea titulat *Blockchain for digital government* (2019), que recomana, en el mateix sentit que la Resolució del Parlament Europeu, de 3 d'octubre de 2018, tantes vegades citada, fer proves pilot d'aquesta tecnologia.

En aquest sentit, el Parlament Europeu ha declarat que la dita tecnologia de registre distribuït, i, en concret, la de les cadenes de blocs, constitueix un instrument idoni per capacitar els ciutadans donant-los l'oportunitat de controlar les seves pròpies dades i decidir quines volen compartir en el registre, com també la capacitat d'escollir qui més pot veure-les (considerant A i apt. 28 Resolució de 3 d'octubre de 2018, citada *supra*). A més, el Parlament subratlla que la Unió Europea no ha de regular *per se* les TRDs sinó que ha d'eliminar els impediments a la seva aplicació, específicament els de la cadena de blocs (Resolució precitada, considerant A i apt. 68).

Exposat aquest context, pel que fa a protecció de les dades, les comunitats autònomes tindran en compte, quan estableixin normativament un servei d'identificació electrònica davant la seva Administració, el RGPD i la completa legislació estatal al respecte, assegurant en aquest camp una protecció efectiva. Precisament, una mostra de les bases estatals en la matèria són els nous apartats 3 dels articles 9 i 10 LPACAP, introduïts pel Reial decret llei 14/2019, que contenen mesures limitatives de la ubicació territorial dels recursos tècnics i de la transferència internacional de dades quan es tracti de la gestió dels sistemes d'identificació i de signatura electròniques dels interessats davant les administracions públiques previstos als apartats 2.c d'ambdós articles. Sobre aquesta qüestió ens remetem a l'anàlisi que hem efectuat dels dits apartats en el DCGE 6/2019 (FJ 5).

El Reglament eIDAS també té present la protecció de les dades personals de forma constant al llarg de tot el seu text (considerant 11 i art. 5). Per la seva part, la Resolució del Parlament Europeu, de 3 d'octubre de 2018, abans esmentada, demana a la Comissió Europea que promogui projectes de

protecció de dades que garanteixin la sostenibilitat de les plataformes TRD (apt. 45). Pel que fa a això, cal indicar que en les modalitats d'aplicació de la tecnologia de registre distribuït hi ha diverses possibilitats tècniques per excloure determinades informacions, entre elles les dades personals, mantenint-les fora dels blocs que es creen i es tanquen, la qual cosa podria també facilitar el compliment del dret a l'oblit digital (en el sentit de la Sentència del Tribunal de Justícia de la Unió Europea, Gran Sala, de 13 de maig de 2014, assumpte C-131/12). A més la informació que hi circula, tot i no ser absolutament anònima, es defineix com a «pseudònima» (definit així a la Resolució del Parlament Europeu, de 3 d'octubre de 2018 —considerant D i apt. 28—, i no prohibit per l'art. 5.2 Reglament eIDAS), formada per un conjunt de caràcters xifrats, que permeten autenticar la identitat sense difondre-la.

Quant a la seguretat o fiabilitat de les dades, són nombrosos els estudis que descriuen aquesta tecnologia com a molt segura entre les existents, a partir de les seves característiques, particularment de la seva immutabilitat, transparència i descentralització. Així, es dona per fet que les diferents variants de la TRD, incloent-hi la *blockchain*, superen el nivell «substancial» que requereix el Reglament eIDAS (com ara els abans indicats sistemes d'identificació electrònica d'Estònia, qualificats de nivell de seguretat alt, segons consta en la llista dels notificats a la Comissió Europea d'acord amb l'article 9.1 Reglament eIDAS). Igualment, el Parlament Europeu, en la Resolució de 3 d'octubre de 2018, ja citada, entre els avantatges de les TRDs destaca la garantia de la integritat de les dades i la capacitat d'oferir «una pista de auditoria a prueba de manipulaciones», que permet nous models d'administració pública i «ayuda a lograr una mejor seguridad» (considerant G).

A l'últim, pel que fa a la ciberseguretat de les xarxes i comunicacions electròniques, l'esmentada institució parlamentària europea assumeix que els

ciberatacs tenen un menor impacte en les cadenes de blocs, enteses com les solucions de TRD que emmagatzemen totes les transaccions individuals en blocs que s'uneixen entre si en ordre cronològic per crear una cadena que garanteix la seguretat i la integritat de les dades, ja que els atacs han d'afectar moltes còpies en comptes d'una versió centralitzada (considerants I i J). Del mateix parer és l'Acord del Govern de la Generalitat pel qual s'aprova l'Estratègia *blockchain* de Catalunya, que considera que la ciberseguretat és intrínseca a aquesta tecnologia, la qual es pot configurar de forma resilient davant els atacs externs (annex, apt. 2.1).

A banda d'això, la regulació autonòmica haurà de tenir en compte, com hem dit, l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica, aprovat pel Reial decret 3/2010 i dictat a l'empara de l'article 149.1.18 CE, on hi ha indicacions precises sobre els requisits de seguretat (art. 11, 27 i annex II, 4 a 6).

Per tant, la disposició addicional sisena.1 LPACAP opta per la solució més lesiva per a les competències autonòmiques. A més, conté una regulació preventiva que prohibeix de forma indefinida una concreta tecnologia (la TRD), la utilització o no de la qual correspon a una decisió de la Generalitat en l'àmbit de l'Administració catalana i a les relacions digitals que manté amb els ciutadans, a l'empara de les seves competències ex article 159 EAC.

El legislador estatal introdueix aquesta prohibició sense ser estrictament necessària o idònia. Tampoc no explicita suficientment les raons que justifiquen dictar una norma prohibitiva d'aquesta mena, en comptes de fixar, podent-ho fer, un marc regulador bàsic, que concreti o afegeixi requisits addicionals de seguretat o de protecció de dades als que ja ordenen el Reglament eIDAS i el Reglament europeu de protecció de dades, per evitar els eventuais problemes que l'esmentat preàmbul del Reial decret llei apunta sense detallar. Es tracta d'un ús espuri i desproporcionat del títol

competencial de l'article 149.1.18 CE per suplir una mancança que en realitat és atribuïble al mateix Estat, que no s'ha dotat d'un marc regulador bàsic.

En altres paraules, l'Estat, en la mesura que no exerceix la seva competència per fixar les bases en aquesta submatèria i, simultàniament, impedeix a la Generalitat que organitzi els seus serveis segons l'opció tecnològica que consideri més òptima, actua de manera poc respectuosa amb el principi de lleialtat institucional que ha de regir en les relacions de cooperació i de col·laboració entre l'Estat i la Generalitat (art. 3 EAC). Així, l'exercici o l'absència d'actuació quant a les competències pròpies no pot obstaculitzar la legítima actuació d'un altre poder o una altra administració pública que compta també amb capacitats reconegudes per incidir en un determinat àmbit sectorial que queda blocat per la interferència del primer (en aquesta línia, DCGE 11/2012 i 12/2012, ambdós de 22 d'agost, FJ 3 i 2.5, respectivament, i 12/2017, d'11 d'octubre, FJ 3). De manera semblant es pronuncia la doctrina constitucional, quan recorda que el principi de lleialtat institucional, tot i no estar expressament reconegut a la Constitució, és essencial i d'obligatòria observança en les relacions entre les diverses instàncies territorials i comporta el deure de respecte de les competències mútues entre les diverses administracions i òrgans públics (STC 85/2016, de 28 d'abril, FJ 5).

Fins a l'actualitat, l'absència de regulació bàsica s'ha resolt, des de la constitució de les comunitats autònomes, en favor de l'exercici de la seva autonomia normativa, si bé aquestes havien d'inferir de l'ordenament jurídic vigent quines eren les bases que havien de respectar (per tots, STC 32/1981, FJ 6, i DCGE 1/2017, FJ 3.4, citats). En cap cas, però, la inactivitat de l'Estat ha conduït a la prohibició de la potestat legislativa de les comunitats autònomes, quan tenien competències en un determinat àmbit.

En conseqüència, per les raons exposades, l'article 3.tres del Reial decret llei 14/2019, en l'apartat primer de la nova disposició addicional sisena que afegeix a la LPACAP, vulnera les competències de la Generalitat ex article 159 EAC i no està emparat per l'article 149.1.18 CE.

Seguidament, examinarem l'apartat segon de la disposició addicional sisena LPACAP, introduïda per l'article 3.tres RDL 14/2019, que atribueix a l'Administració general de l'Estat el paper d'autoritat intermèdia que exerceix les funcions que correspongui per garantir la seguretat pública, per a qualsevol sistema d'identificació basat en TRD que prevegi la legislació estatal.

D'entrada, ja s'observa que aquest apartat, que es presenta com una norma aparentment clara, mostra diverses incoherències de caràcter essencial, com veurem a continuació.

Primerament, la seva formulació no es concilia amb el mandat constitucional de l'article 86 CE. Això és així perquè, en clau de futur i sense determinar quan, estableix que qualsevol sistema d'identificació i de signatura electròniques basat en tecnologies de registre distribuït que prevegi la legislació que aprovi l'Estat al seu dia haurà de disposar que l'Administració central actuï com a autoritat intermèdia.

Com és evident, no es tracta d'una mesura concreta de caràcter immediat, com exigeix la jurisprudència constitucional per admetre la seva aprovació mitjançant una norma d'origen governamental (STC 332/2005, de 15 de desembre, FJ 7, i STC 96/2014, de 12 de juny, FJ 7); és a dir, les mesures incorporades a un decret llei han de modificar de manera instantània la situació jurídica existent a fi de fer-hi front (STC 39/2013, de 14 de febrer, FJ 9, i 1/2012, de 13 de gener, FJ 11, entre d'altres).

A més a més no compleix, amb caràcter general, amb el pressupòsit constitucional d'extraordinària i urgent necessitat, tal com l'hem exposat a l'esmentat DCGE 6/2019 (FJ 2) i reiterat al principi del fonament jurídic segon (apt. 1).

S'observa, a més, que l'apartat segon de la disposició addicional sisena examinat és inaplicable i intranscendent, des del moment que porta causa d'uns sistemes que, per mandat de la mateixa norma, no són admissibles ni poden implementar les administracions públiques, perquè l'Administració de l'Estat no els autoritza.

Per tant, des d'aquesta perspectiva, l'article 3.tres RDL 14/2019, en l'apartat 2 de la disposició addicional sisena que introdueix en la LPACAP, és inconstitucional, perquè no respecta els requisits del pressupòsit formal habilitant exigint per l'article 86.1 CE per a l'aprovació legítima d'una regulació mitjançant decret llei.

Sens perjudici que ja podríem aturar la nostra anàlisi en aquest punt, cal recordar que l'Estat podria legislar amb caràcter de bàsics els aspectes sobre la seguretat i el dret a la protecció de dades personals que estiguessin relacionats amb la utilització dels sistemes d'identificació i de signatura electròniques davant les administracions públiques basats en *blockchain*, entre altres TRDs. Ara bé, ho ha de fer, en tot cas, d'acord amb la naturalesa que han de tenir les bases com a principis o mínim comú, de manera que deixin marge suficient per permetre l'exercici de les competències de les comunitats autònomes. Aquesta futura regulació, segons el nostre criteri, seguint la jurisprudència constitucional prevalent, hauria d'adoptar, com a regla general, el rang de llei i, com acabem d'assenyalar, ha de permetre que la Generalitat adopti les seves polítiques pròpies dins de l'espai que li correspon d'acord amb l'Estatut.

Dit això, l'apartat 2 de la disposició addicional sisena LPACAP constitueix una mena de declaració programàtica *pro futuro* del contingut d'unes bases encara no concretades.

Així, la dita configuració creiem que és un exemple de mala tècnica legislativa, atès que genera un marc confús i susceptible d'interpretacions diverses: d'una banda, no permet l'examen d'unes eventuais bases perquè no precisa el seu abast ni els seus efectes, i d'altra banda, si s'entengués que, al mateix temps, autoritza una regulació reglamentària, sense necessitat d'una nova llei, no estaria emparada legítimament per la disposició final segona RDL 14/2019, que atorga al Govern i a determinats òrgans administratius de l'Estat la capacitat per dictar les disposicions que siguin necessàries per al desenvolupament i l'execució del que disposa la dita norma.

Per tant, podem concloure que, en sentit estricte, el seu contingut, per si sol, no manifesta tantes d'inconstitucionalitat, en espera del coneixement precís de la intervenció futura del legislador estatal quan exerceixi la seva capacitat per dictar les bases, i sens perjudici del resultat del seu examen si s'escau, però sí que hem de remarcar la seva deficient tècnica legislativa.

Arribats a aquest punt, i ja com a mer *obiter dictum* sobre l'element principal del contingut que prescriu en clau de regulació de futur de l'apartat 2 de la disposició addicional sisena LPACAP, és a dir, sobre la previsió d'una autoritat intermèdia, es poden formular les següents consideracions.

Esdevé d'interès assenyalar que una de les singularitats principals que configuren les tecnologies de registre distribuït, incloent-hi les cadenes de blocs, que són les més habituals, és, tal com hem exposat abans, la seva naturalesa descentralitzada i consensuada. Aquesta premissa suposa que dues parts interessades poden efectuar operacions directament entre elles

sense necessitat d'un tercer de confiança o, el que és el mateix, sense intermediaris que tinguin posicions de control en la seva organització. Per aquest motiu, quan es tracta de TRDs, en principi no tindria sentit preveure de forma general l'establiment d'una autoritat intermèdia, cosa que contradiria el criteri anterior, si no és per a determinades aplicacions de la dita tecnologia, que poden matisar aquest tret característic i definidor, tal com hem apuntat a l'inici de l'apartat 2 d'aquest fonament jurídic. Val a dir, quant al contingut de l'apartat 2 de la disposició addicional sisena LPACAP que, atesa la seva indefinició o manca de precisió, no es pot entreveure a què es refereix amb l'expressió «autoritat intermèdia». És a dir, no se sap en quin moment del procés d'identificació intervindria aquesta autoritat, com tampoc es poden determinar quines funcions tindria atribuïdes ni els efectes que comporta la seva constitució per al disseny, la implementació i l'operativitat dels sistemes dels articles 9.2.c i 10.2.c LPACAP als quals afecta.

Sigui com sigui, quant a l'atribució de l'exercici de funcions per garantir la seguretat pública a una autoritat estatal, en l'àmbit de l'administració digital, cal recordar que les dites funcions, si escau, s'inclourien dins de la seguretat de les xarxes i les comunicacions electròniques, particularment en relació amb la seva fiabilitat i que, per tant, en principi, si fossin necessàries, podrien correspondre a la Generalitat, en virtut de les competències assumides per l'article 159 EAC, com hem anat exposant en aquest Dictamen i en el DCGE 6/2019 (FJ 3).

6. Per finalitzar aquest fonament jurídic, respecte de l'apartat 2 de la disposició final primera RDL 14/2019, hem d'arribar a la mateixa conclusió d'inconstitucionalitat i d'antiestatutarietat, per connexió, a la que hem arribat amb relació a l'apartat tres de l'article 3 RDL 14/2019, que hem considerat que no troba empara en els títols competencials de l'article 149.1.18 i .29 CE

i que vulnera les competències de la Generalitat assumides per l'article 159 EAC.

Atesos els raonaments continguts en els fonaments jurídics precedents, formulem les següents

CONCLUSIONS

Primera. El Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions és contrari a l'article 86.1 CE, perquè no compleix el requisit constitucional de l'extraordinària i urgent necessitat.

Adoptada per unanimitat.

Segona. L'article 3.u i .dos del Reial decret llei 14/2019, en la redacció que dona als articles 9.2.c i 10.2.c de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, concretament en l'incís, «amb l'autorització prèvia de la Secretaria General d'Administració Digital del Ministeri de Política Territorial i Funció Pública, que només es pot denegar per motius de seguretat pública, amb l'informe previ vinculant de la Secretaria d'Estat de Seguretat del Ministeri de l'Interior. L'autorització s'ha d'emetre en el termini màxim de tres mesos. Sense perjudici de l'obligació de l'Administració General de l'Estat de resoldre dins del termini, la manca de resolució de la sol·licitud d'autorització s'entén que té efectes desestimatoris», vulnera les competències de la Generalitat de l'article 159 EAC i no troba empara en l'article 149.1.18 i .29 CE. Per connexió, la disposició transitòria primera, apartat 1, i la disposició final

primera, apartat 2, del Reial decret llei 14/2019 també les vulneren i tampoc no troben empara en els preceptes constitucionals citats.

Adoptada per unanimitat.

Tercera. L'article 3.u i .dos del Reial decret llei 14/2019, en l'obligació que incorpora als articles 9.3 i 10.3 de la Llei 39/2015 de situar «en territori espanyol» els recursos tècnics necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió dels sistemes previstos en els articles 9.2.c i 10.2.c de l'esmentada Llei, com també, per connexió, la disposició transitòria primera, apartat 2, del mateix Reial decret llei, són contraris al principi de lliure circulació de dades previst a l'article 1 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, quant al tractament de dades personals i a la lliure circulació d'aquestes i pel qual es deroga la Directiva 95/46/CE.

Adoptada per unanimitat.

Quarta. L'article 3.tres del Reial decret llei 14/2019, en la nova disposició addicional sisena que afegeix a la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, vulnera les competències de la Generalitat ex article 159 EAC i no troba empara en l'article 149.1.18 i .29 CE. Per connexió, la disposició final primera, apartat 2, del Reial decret llei 14/2019 també les vulnera i tampoc no troba empara en els preceptes constitucionals citats.

Adoptada per unanimitat.

Cinquena. L'article 6.u del Reial decret llei 14/2019, en la redacció que dona al primer paràgraf de l'apartat 6 de l'article 4 de la Llei 9/2014, de 9 de maig, general de telecomunicacions, quant a la facultat d'«intervenció» que atribueix a l'Estat, és inconstitucional perquè vulnera l'article 9.3 CE, ja que no compleix les exigències de qualitat normativa que hauria d'observar una

lleï susceptible de produir ingerències en l'exercici dels drets fonamentals i les llibertats públiques.

Adoptada per unanimitat.

Sisena. La resta de preceptes examinats del Reial decret llei 14/2019 no són contraris a l'Estatut ni a la Constitució.

Adoptada per unanimitat.

Aquest és el nostre Dictamen, que pronunciem, emetem i signem al Palau Centelles en la data indicada a l'encapçalament.