D I C T A M E N 6/2019, de 30 de desembre, 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 Fernàndez, 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 pel Govern de la Generalitat 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 (BOE núm. 266, de 5 de novembre de 2019).

PALAU CENTELLES
Baixada de Sant Miquel, 8 - 08002 Barcelona
Tel. + 34 933 176 268 Fax + 34 933 181 720
consell@cge.cat

A N T E C E D E N T S

1. El dia 2 de desembre de 2019 va tenir entrada en el Registre del Consell de Garanties Estatutàries un escrit del conseller d'Acció Exterior, Relacions Institucionals i Transparència, de 2 de desembre (Reg. núm. E2019000629), 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 comunicava al Consell l'acord del Govern de 26 de novembre de 2019, de sol·licitud d'emissió de dictamen sobre l'adequació a l'Estatut i a la Constitució dels articles 1, 2, 3, 4, 6, 7, la disposició addicional única i, per connexió, les disposicions transitòries primera i segona i la disposició final primera 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.

El sol·licitant demana 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.

2. El Consell de Garanties Estatutàries, en la sessió del dia 3 de desembre de 2019, després d'examinar la legitimació i el contingut de la sol·licitud, de conformitat amb els articles 23 a 25, apartats 1 a 3, LCGE, va acordar la seva admissió a tràmit i es va declarar competent per emetre el dictamen corresponent. A continuació, es va acordar realitzar una ponència conjunta dels consellers Jaume Vernet Llobet i Francesc de Paula Caminal Badia i del conseller secretari Àlex Bas Vilafranca.

3. En la mateixa sessió, a l'empara de l'article 25 LCGE, apartat 4, i de l'article 35, apartat 1, del Reglament d'organització i funcionament del Consell, va acordar adreçar-se al Govern a fi de sol·licitar-li la informació i la documentació complementàries de què disposés amb relació a la matèria sotmesa a dictamen.

4. En data 11 de desembre de 2019 es va rebre en el Registre del Consell un escrit del conseller d'Acció Exterior, Relacions Institucionals i Transparència (Reg. núm. E2019000657) que adjuntava com a documentació complementària un informe de l'Assessoria Jurídica del Departament de Polítiques Digitals i Administració Pública, de 18 de novembre de 2019, i unes notes relatives a l'impacte en l'àmbit de l'Administració digital i el procediment administratiu comú del Reial decret llei 14/2019, elaborades per l'Oficina d'Innovació i Administració Digital.

5. Finalment, després de les corresponents sessions de deliberació del Consell, el dia 30 de desembre de 2019 ha tingut lloc la votació i l'aprovació d'aquest Dictamen, d'acord amb el que preveuen els articles 31.1 LCGE i 38 del Reglament d'organització i funcionament del Consell.

F O N A M E N T S J U R Í D I C S

Primer. L'objecte del Dictamen

D'acord amb el que s'ha exposat en els antecedents, el Govern demana el parer del Consell, amb caràcter previ a la interposició, si escau, d'un recurs d'inconstitucionalitat davant del Tribunal Constitucional, a l'empara dels articles 16.2.*a* i 31 de la LCGE, amb relació a diversos preceptes 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 (en endavant, RDL 14/2019 o Reial decret llei).

En aquest primer fonament jurídic ens limitarem a resumir de manera breu el contingut del Reial decret llei, recollint també succintament els dubtes generals que el Govern expressa en la seva sol·licitud respecte dels preceptes que han de ser l'objecte del nostre pronunciament. La descripció, el detall de les qüestions plantejades per l'escrit de petició del dictamen, l'examen i la conclusió sobre les normes concretes els diferim als fonaments jurídics següents, segons l'estructura que tot seguit enunciarem. El motiu d'aquest petit canvi en la sistemàtica de la nostra anàlisi, en el sentit d'alleugerir aquest fonament jurídic, respon a la complexitat tècnica de la matèria i a l'heterogeneïtat de les mesures de la norma, la qual si és tractada en diferents parts segregades per raó de l'àmbit a què fan referència facilita la claredat expositiva.

1. El Reial decret llei objecte de dictamen, 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.

El seu contingut és heterogeni i comprèn un feix divers de 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 sistemes d'informació (cap. V, art. 7).

2. L'escrit de petició del Dictamen qüestiona, en primer lloc, l'adequació de l'instrument normatiu emprat pel Govern de l'Estat en la mesura que, al seu parer, no estarien acreditades les raons d'extraordinària i urgent necessitat que el justifiquen i que ordena àmbits que no són susceptibles de ser regulats mitjançant reial decret llei.

Fetes aquestes observacions sobre l'ús de la figura de l'instrument normatiu emprat, el Govern de la Generalitat entén que les mesures incorporades per la norma podrien incidir en les competències de la Generalitat en matèria de comunicacions electròniques, organització de la seva Administració i règim jurídic i procediment de les administracions públiques catalanes i en matèria de seguretat pública, reconegudes en els articles 140.7, 150, 159 i 164 EAC, respectivament. Així mateix, qüestiona que la intervenció administrativa que s'atribueix al Govern de l'Estat en aquest àmbit de les xarxes i els serveis de comunicacions electròniques sigui susceptible de ser duta a terme sense autorització judicial, amb la conseqüent potencial afectació de drets fonamentals.

L'escrit de petició recull una descripció del contingut dels cinc capítols del RDL 14/2019, acompanyada de l'explicació dels dubtes que alguns dels seus preceptes susciten, tot i que finalitza amb una sol·licitud genèrica de pronunciament sobre l'adequació a la Constitució i a l'Estatut d'autonomia dels articles 1, 2, 3, 4, 6 i 7, de la disposició addicional única i, per connexió, de les disposicions transitòries primera i segona i la disposició final primera.

Respecte dels preceptes citats per la sol·licitud de dictamen, aquest Consell examinarà, tal com ho estableix la nostra Llei (art. 24 LCGE), així com la pràctica consolidada en la nostra funció consultiva i la jurisprudència constitucional mateixa, les normes respecte de les quals s'aporti una mínima

justificació quant a les raons de la seva possible inconstitucionalitat o antiestatutarietat.

3. D'acord amb això anterior, per donar resposta a la petició, en el fonament jurídic segon analitzarem el compliment per part de la norma dictaminada dels requisits constitucionals del decret llei *ex* article 86.1 CE.

Seguidament, en el fonament jurídic tercer examinarem les mesures en matèria de documentació nacional d'identitat establertes en els articles 1 i 2 RDL 14/2019, pels quals es modifiquen 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), així com les mesures d'identificació i signatura electrònica davant les administracions públiques previstes a l'article 3.u i .dos RDL 14/2019, en allò referit 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 (en endavant, LPACAP) i en la disposició transitòria primera, apartat 1, del Reial decret llei.

A continuació, en el fonament jurídic quart analitzarem, d'una banda, les mesures en matèria de telecomunicacions regulades en l'article 6.u i .cinc RDL 14/2019, que modifica els articles 4.6 i 81.1 de la Llei 9/2014, de 9 de maig, general de telecomunicacions (en endavant, LGTEL), respectivament, i l'article 6.dos, pel qual s'afegeix a l'esmentada LGTEL un nou apartat 3 al seu article 6, juntament amb la disposició addicional única del Reial decret llei, sobre comunicació de les xarxes de comunicacions electròniques en règim d'autoprestació de les administracions públiques.

I, d'una altra, en aquest mateix fonament abordarem les mesures per reforçar la coordinació en matèria de seguretat de les xarxes i els sistemes d'informació previstes a l'article 7 RDL 14/2019, mitjançant el qual

s'incorpora un nou apartat 3 a l'article 11 del Reial decret llei 12/2019, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació (en endavant, Reial decret llei 12/2019).

Finalment, en el fonament jurídic cinquè i darrer tractarem les qüestions plantejades pel peticionari relatives al dret a la protecció de dades personals pel que fa a l'article 3.u i .dos RDL 14/2019 en relació amb l'addició d'un nou apartat 3 als articles 9 i 10 LPACAP i, per connexió, el seu règim transitori (disp. trans. primera, apt. 2 RDL 14/2019); l'article 4.u pel qual s'afegeix un nou article 46 bis a la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic (en endavant, LRJSP) i el seu règim transitori (disp. trans. segona RDL 14/2019), i l'article 4.dos, que modifica l'article 155 LRJSP.

Pel que fa a la disposició final primera, relativa als títols competencials que habiliten la norma dictaminada, ens hi referirem, si escau, i per connexió, quan analitzem els preceptes concrets en els esmentats fonaments jurídics.

Segon. L'examen del compliment dels requisits constitucionals del decret llei de l'article 86.1 CE i la seva aplicació al Reial decret llei 14/2019

Ens correspon en aquest fonament jurídic examinar prèviament el cànon de constitucionalitat del decret llei, d'acord amb l'article 86.1 CE, per aplicar-lo posteriorment als preceptes qüestionats de la norma objecte de dictamen. Per això, efectuarem, de primer, una anàlisi succinta de la configuració d'aquest tipus de norma, àmpliament estudiada per aquest Consell en altres dictàmens. També farem un recordatori breu de la jurisprudència constitucional corresponent, a bastament citada en els nostres pronunciaments consultius.

Com ja hem afirmat amb anterioritat i de forma reiterada en diversos dictàmens, el decret llei es configura com una norma jurídica amb rang de llei, dictada pel Govern amb caràcter excepcional. Suposa l'atribució de l'exercici de la potestat legislativa ordinària del Parlament al Govern, exceptuant d'aquesta manera el monopoli parlamentari de la potestat legislativa (art. 66.2 CE). Per aquesta raó, la utilització d'aquest tipus de disposicions ha de ser duta a terme de forma restrictiva i, conseqüentment, ha de respectar de manera inexcusable els límits formals i materials que preveu l'article 86.1 CE (per tots, DCGE 5/2019, de 23 de juliol, FJ 3).

Amb relació a aquests requisits, tant pel que fa al pressupòsit formal habilitant com als límits per raó del seu objecte (aspectes, ambdós, demanats a la sol·licitud de dictamen), ens remetem a la nostra doctrina consultiva consolidada (entre d'altres, DCGE 5/2012, de 3 d'abril, FJ 2; 6/2012, d'1 de juny, FJ 2; 25/2014, d'11 de desembre, FJ 3, i més recentment DCGE 5/2019, FJ 3). Per tant, en nom de la brevetat i la simplificació, en resumirem el seu contingut, en allò que ara més ens interessa. Simultàniament, també recordarem, sense fer-ne citació literal, la jurisprudència del Tribunal Constitucional relativa als decrets llei (en particular, STC 34/2017, d'1 de març, on es fa una síntesi de la seva interpretació). Sobre aquest punt, sigui dit d'entrada, en la tasca d'escrutini de la presència del pressupòsit habilitant del decret llei, aquest Consell ha estat més exigent que la jurisprudència constitucional i ha qüestionat repetidament l'ús excessiu d'aquesta figura normativa, cosa «que no deixa de ser preocupant des de la perspectiva constitucional, per molt que es prevegi una sessió de convalidació parlamentària» (per tots, DCGE 5/2019, FJ 3).

1. En primer lloc, procedirem, per tant, a l'examen de l'existència o no de l'extraordinària i urgent necessitat, així com també de la connexió de sentit

entre les mesures aprovades i la situació a la qual pretén donar solució, que són elements, ambdós, del pressupòsit formal habilitant.

Respecte d'aquesta qüestió, la sol·licitud de dictamen expressa els seus dubtes sobre la inadequació del Reial decret llei, en tant que «no s'acrediten degudament les raons d'extraordinària i urgent necessitat que el justifiquen». A més, indica que el preàmbul únicament esmenta els riscos des de la perspectiva de la seguretat pública, «quan aquests ja formen part de la pròpia estructura de l'esquema de seguretat», aprovada amb anterioritat.

A) Com dèiem en el fonament jurídic tercer del DCGE 25/2014, la naturalesa extraordinària de la necessitat ha estat interpretada pel Tribunal Constitucional i pel Consell com el supòsit excepcional en el qual una situació conjuntural de difícil previsió requereix una intervenció normativa immediata per part del Govern per fer front als objectius de governabilitat (per totes, STC 137/2011, de 14 de setembre, FJ 4, i també DCGE 15/2014, de 3 de juliol, FJ 2.3). És suficient, pel que fa a l'abast de la necessitat, que aquesta s'origini en les tasques concretes i habituals del Govern i no cal que siguin necessitats extremes o absolutes (STC 6/1983, de 4 de febrer, FJ 5).

La doctrina jurisprudencial s'ha mostrat, en termes generals, més procliu a la validació del decret llei, quan es tracta «de las actuaciones desarrolladas en los ámbitos de la política social y económica» (STC 68/2007, de 28 de març, FJ 12) o en circumstàncies d'especial conjuntura econòmica, que exigeixen una resposta normativa urgent, sempre que aquestes hagin estat degudament exposades i justificades en el text de la disposició. Tanmateix, no n'hi ha prou amb partir de conjectures, sinó que cal verificar-ho sobre una concreta situació fàctica, que ha de ser evidenciada pel Govern de l'Estat.

En aquest sentit, el Tribunal ha insistit que s'han de tenir presents «las situaciones concretas y los objetivos gubernamentales» (STC 329/2005, de 15 de desembre, FJ 5), que han conduït a l'emissió d'un decret llei específic. El requisit consistent a justificar de forma explícita i raonada l'existència del pressupòsit habilitant és una exigència que no pot decaure en cap cas, ni tan sols quan s'inscriu en situacions de crisi econòmica (DCGE 16/2013, de 15 de novembre, FJ 3.3), circumstància que, sigui dit d'avançada, tampoc no es produeix en el supòsit que estem dictaminant, el qual, com veurem més endavant, afecta altres matèries, singularment la seguretat pública en diferents àmbits, com indica el títol mateix de la norma.

Precisament la manca de justificació de la necessitat ha fonamentat el viratge de la jurisprudència constitucional cap a una concepció més estricta de la utilització del decret llei, que, en algunes ocasions, ha conduït cap a la inconstitucionalitat de la disposició governativa examinada i que té com a exponent clar la STC 68/2007, en la qual el Tribunal no admet la fonamentació de l'extraordinària i urgent necessitat mitjançant una clàusula ritual, força abstracta. Per contra, exigeix que el Govern expliqui en concret i raoni suficientment per què ha considerat que es dona aquest tipus de situació, per molt que l'apreciació inicial de la seva existència es consideri un judici polític que correspon efectuar al Govern (FJ 10), el qual no ha de fer impossible el control de constitucionalitat. Aquesta línia ha estat seguida posteriorment en altres pronunciaments (com ara les STC 150/2017, de 21 de desembre; 125/2016, de 7 de juliol; 29/2015, de 19 de febrer, i 137/2011, de 14 de setembre). Més recentment, en la STC 61/2018, de 7 de juny, el Tribunal ha insistit novament que s'ha de fugir de «fórmulas rituales o genéricas» que no permeten justificar la necessitat (FJ 7).

Atès que en la determinació d'allò que constitueix una necessitat extraordinària els poders públics gaudeixen d'un marge de discrecionalitat raonable, la funció de control d'aquest Consell s'ha de limitar a verificar que

els motius siguin suficientment explícits, raonats i mancats d'aparença d'arbitrarietat (per tots, DCGE 5/2019, FJ 3, i 5/2015, de 20 d'abril, FJ 2), sotmetent-los a un test formal de raonabilitat (DCGE 6/2012, FJ 2; 11/2012, de 22 d'agost, FJ 5, i 15/2014, FJ 2.3).

Com dèiem en el DCGE 6/2012, i acabem de recordar, el pressupòsit habilitant «ha de ser verificable i, per tant, els motius de la seva justificació han de constar de manera expressa» (FJ 2). Així doncs, la revisió d'aquest Consell ha de constatar l'existència d'una «exposició motivada i fonamentada de la justificació per la qual es recorre a la via del decret llei, per tal de descartar el seu ús abusiu o arbitrari» (DCGE 15/2014, FJ 2.3).

Per efectuar la tasca de verificació, el Tribunal Constitucional exigeix que la justificació es desprengui en tot cas de l'anàlisi conjunta del preàmbul de la norma, i dels documents que s'adjunten al seu expedient de tramitació, així com del debat de convalidació del decret llei corresponent, cosa que examinarem seguidament.

De l'anàlisi de les dades de què disposem respecte del RDL 14/2019 es constata que ni en el preàmbul ni en el debat de convalidació davant la Diputació Permanent del 27 de novembre de 2019 (DSCD núm. 14), encara en els darrers dies de la XIII legislatura, no s'acredita de forma explícita i raonada una justificació suficient per avalar la constitucionalitat del Reial decret llei *ex* article 86.1 CE, com ho exigeix la jurisprudència del Tribunal Constitucional (per totes, STC 11/2002, de 17 de gener, FJ 4). Així, entenem que no es pot inferir l'existència d'una extraordinària necessitat, tant pel que fa a la norma en el seu conjunt com específicament respecte de cadascun dels preceptes que s'hi contenen, com exposem a continuació.

En el preàmbul es mencionen dues situacions de naturalesa diversa que, eventualment, podrien justificar la necessitat de dictar un decret llei.

D'una banda, a l'inici, de forma general s'afirma que «[l]a societat actual requereix adaptacions en l'esfera digital que exigeixen una traducció en el pla normatiu. El desenvolupament i l'ús de les noves tecnologies i les xarxes de comunicacions per part de les administracions públiques s'està accelerant. Això exigeix establir sense demora un marc jurídic que garanteixi l'interès general i, en particular, la seguretat pública» (apt. I, par. primer). Aquesta diagnosi no és nova, com reconeix el proemi del Reial decret llei quan esmenta el caràcter estratègic de la seguretat pública, avalat per la Llei 36/2015, de 28 de setembre, de seguretat nacional. La dita estratègia de seguretat nacional va ser aprovada pel Reial decret 1008/2017, d'1 de desembre (apt. I, par. segon i tercer).

La mateixa argumentació, i amb unes paraules semblants, també de caràcter genèric i abstracte, es reprodueix posteriorment en l'apartat dedicat a la justificació competencial de la norma quan se sosté que «les mesures que conté aquest Reial decret llei tenen com a finalitat incrementar l'estàndard de protecció de la seguretat pública davant les amenaces creixents que planteja l'ús de les noves tecnologies» (apt. VI, par. cinquè).

D'altra banda, es diu igualment que «[e]ls recents i greus esdeveniments esdevinguts a part del territori espanyol han posat de relleu la necessitat de modificar el marc legislatiu vigent per fer front a la situació. Aquests fets demanen una resposta immediata per evitar que es reprodueixin successos d'aquesta índole amb l'establiment d'un marc preventiu amb aquesta finalitat» (apt. I, par. sisè) i es vincula amb la disquisició anterior, sobre les ciberamenaces, quan s'hi afegeix que «i sempre en vista dels últims successos en territori espanyol» (apt. VI, par. cinquè).

Per tant, es fa referència de passada a una greu situació indeterminada en una part de l'Estat i a uns successos, sense concretar ni els fets produïts, ni

on precisament s'ha ocasionat aquesta afectació dels drets dels ciutadans i de la seguretat pública.

A més a més, quan el preàmbul exposa les diverses parts del contingut de la norma tampoc no esmenta perquè calen els canvis que incorpora, des de la perspectiva de la seva extraordinària necessitat.

En la presentació del Reial decret llei per part de la ministra d'Economia i Empresa en funcions durant l'acte de convalidació abans esmentat, tampoc no es van aclarir cap d'aquests dubtes, ja que no va tractar en cap moment les raons que avalaven una extraordinària necessitat, ni tampoc no va concretar la situació que es pretenia afrontar amb aquesta disposició, ni tan sols la localització dels fets que meritaven una actuació normativa estatal extraordinària.

Arribats a aquest punt, considerem que la utilització per part del preàmbul de fórmules rituals i abstractes, com ara que la societat actual exigeix una adaptació en l'esfera digital o que l'acceleració en l'ús de les noves tecnologies per part de l'Administració exigeix establir un marc jurídic que garanteixi l'interès general, o l'ús d'expressions ambigües o imprecises, tals com «greus esdeveniments», «successos d'aquesta índole», sense cap altra concreció, tampoc en el debat de la convalidació del decret llei, no permeten albirar la situació, bé conjuntural o bé estructural, a la qual pretén donar resposta el Reial decret llei, ni, per descomptat, concretar si té el caràcter d'excepcional, greu, rellevant i imprevisible que habilitaria l'ús de la potestat legislativa extraordinària del Govern. En conseqüència, aquesta aparent justificació no és admissible constitucionalment per acreditar el requisit habilitant per dictar el Reial decret llei.

Tot això anterior es fa encara més palès tenint en compte que la disposició legislativa dictaminada comprèn la modificació de diversos àmbits materials

(principalment, documentació nacional d'identitat, administració digital, contractació pública, telecomunicacions i protecció de dades) i dels seus corresponents instruments normatius, que haurien necessitat, al nostre parer, d'una fonamentació específica i singularitzada. Com hem sostingut recentment en el DCGE 5/2019 (FJ 3), «si les mesures que conté un decret llei són diverses […], les situacions concretes d'urgència i necessitat que justifiquen la seva adopció també són susceptibles de ser-ho (STC 199/2015, FJ 5, i 61/2018, FJ 6, i, aplicant aquesta doctrina, DCGE 11/2012, FJ 5, o 5/2015, FJ 2)».

Respecte a la precitada nota d'imprevisibilitat, el fet que el Reial decret llei inclogui un conjunt de reformes legislatives recents no abona tampoc aquesta idea. Les temàtiques distintes que tracta la norma que dictaminem, ja havien estat discutides en seu parlamentària, si bé no plenament en la direcció suara proposada. En aquest sentit, la STC 137/2011 diu que «la situación […] que se pretende afrontar en el precepto recurrido ya había sido apreciada y puesta de manifiesto con anterioridad en otros instrumentos normativos que precedieron al Real Decreto-ley» (FJ 7).

En conseqüència, és palmària la insuficiència de la deguda justificació de l'existència d'una situació greu, rellevant, excepcional o imprevisible a la qual fer front i, per tant, del caràcter extraordinari de la necessitat de dictar aquest Reial decret llei.

B) Juntament amb el caràcter extraordinari de la necessitat, el compliment del pressupòsit formal habilitant exigeix la presència de l'element de la urgència. Per caracteritzar-la, la jurisprudència del Tribunal Constitucional ha interpretat que «[e]l fin que justifica la legislación de urgencia no es otro que subvenir a "situaciones concretas de los objetivos gubernamentales que por razones difíciles de prever requieran una acción normativa inmediata en un plazo más breve que el requerido por la vía normal o por el procedimiento de

urgencia para la tramitación parlamentaria de las leyes"» (per totes, STC 137/2011, FJ 4). En un sentit anàleg, la nostra doctrina consultiva entén que «el Govern únicament estaria legitimat per exercir la seva potestat normativa mitjançant decret llei quan per la via de la tramitació parlamentària de naturalesa més urgent no fos raonablement viable o possible assolir els objectius perseguits per l'acció normativa» (DCGE 15/2014, FJ 2.3, que es remet al DCGE 7/2010, de 22 d'abril).

De la mateixa manera que l'extraordinària necessitat, la urgència cal que també sigui justificada de manera motivada i expressa (DCGE 7/2012, de 8 de juny, FJ 3.3). Així, hem recordat els dictàmens del Consell Consultiu (DCC 268, de 31 de maig de 2005, F II, i DCC 292, de 8 d'abril de 2009, F II) en el DCGE 7/2010, de 22 d'abril, on s'afirmava que «la urgent necessitat de proveir de norma reguladora una determinada situació fàctica s'ha d'identificar i concretar en el contingut de les disposicions generals emanades a aquest efecte» (FJ 3). I, en ocasió del nostre pronunciament sobre un Decret llei de la Generalitat, hem afegit que «l'excepcionalitat de la necessitat ha d'anar acompanyada de la constatació, motivada i expressa, que el procediment en seu parlamentària afectaria decisivament, per raons de temps excessiu, l'obtenció de l'efecte o els resultats cercats per les mesures exigides per tal de fer-hi front» (DCGE 17/2013, de 15 de novembre, FJ 2, que recull el DCGE 6/2012, d'1 de juny, FJ 2).

En el supòsit que ens ocupa, i a tall de justificació d'una necessitat urgent, tant en el preàmbul del Reial decret llei (apt. III, par. cinquè) com en la seva presentació davant la Diputació Permanent (DSCD esmentat, p. 14) s'addueix el fet que les cambres es troben dissoltes. Per aquesta raó, el Reial decret llei s'ha convalidat davant la Diputació Permanent i no davant el Ple del Congrés de Diputats. És cert que això és així i, a més, que un govern en funcions no pot presentar projectes de llei per ser tramitats (art. 21.5 de la Llei 50/1997, de 27 de novembre, del Govern), per la qual cosa cal tenir en

compte quan s'iniciarà la nova legislatura (que va tenir lloc el 3 de desembre de 2019, pocs dies més tard de la convalidació) i quan podrà ser efectiva la presentació de projectes de llei per ser debatuts. El Reial decret llei ha entrat en vigor el 6 de novembre, quasi un mes abans d'iniciar-se la XIV legislatura.

D'entrada, i en l'anàlisi de la urgència des de la perspectiva que el procediment legislatiu ordinari no possibiliti cap via per a l'adopció de les mesures sense haver de recórrer a la figura del decret llei, hem de dir que l'especial i específic fet que acabem d'exposar corroboraria en certa manera, i a priori, la utilització d'aquest tipus de norma, ja que ens situa en un cert context d'incertesa temporal i, per tant, d'urgència, pel fet que el Govern no disposaria de cap altre instrument legislatiu per aprovar ràpidament les mesures pertinents per fer front a una justificada necessitat extraordinària. Certament, no podria presentar un projecte de llei perquè les cambres estan dissoltes i, una vegada constituïdes, hauria d'esperar que es constituís un nou Govern per poder-lo presentar. Però això anterior no és, a parer nostre, suficient, pel que es dirà després, per acreditar l'existència de la necessitat urgent, ja que ha de quedar fonamentada la peremptorietat de l'acció legislativa i, per tant, la impossibilitat d'obtenir el mateix resultat mitjançant l'aprovació d'una disposició que segueixi la tramitació ordinària o urgent en les cambres legislatives (DCGE 17/2013, de 15 de novembre, FJ 2).

És il·lustratiu assenyalar, en aquest sentit, que aquest Consell no ha considerat com a fonament acreditatiu d'un supòsit d'urgència la mera hipòtesi de l'exhauriment de la legislatura, atesa la possible convocatòria anticipada d'eleccions. Així, en el DCGE 5/2015, vam declarar que el dit fet conjuntural, «ni que arribi a produir-se, no pot operar com a justificació» (FJ 2.2). Això suposaria, en paraules del precitat Dictamen (interpretant l'art. 64.1 EAC, als nostres efectes aplicable a l'art. 86 CE), una «desnaturalització d'un supòsit previst exclusivament per a situacions que, per la seva caracterització fàctica, generalment sobrevinguda, necessiten una normativa

immediata en bé de l'interès públic», condició «ben distinta i incompatible» amb un recurs per fer front a contextos derivats de decisions o motivacions estrictament polítiques (FJ 3).

Per tant, per efectuar l'escrutini sobre l'existència de la urgència de la situació és necessari no només citar expressament la concreta situació que es vol afrontar amb rapidesa, sinó també exposar una fonamentació per part del Govern de l'Estat de quins serien, en el cas que ens ocupa, els perjudicis i obstacles que es derivarien d'esperar la constitució i presentació de projectes de llei, en una tramitació legislativa ordinària, fins i tot a través del tràmit legislatiu d'urgència (STC 68/2007, FJ 12).

Aquest punt s'explicita, de manera molt genèrica i poc motivada, en el preàmbul del Reial decret llei i en la seva presentació en el debat de convalidació. Així, l'única referència que s'efectua en el primer és al fet que la introducció de les mesures a través d'un projecte de llei no es pot fer en el moment present perquè les cambres estan dissoltes i no se'n pot dilatar l'adopció fins a la Constitució de les Corts Generals perquè, fins i tot amb la utilització aleshores del tràmit d'urgència, «no s'aconseguiria reaccionar a temps» (apt. III. par. cinquè). Per la seva banda, pel que fa al debat de convalidació, la ministra repeteix que es tracta d'una norma urgent «habida cuenta de la celeridad con la que se están produciendo los avances en esta materia y dada la situación política actual, con el Gobierno en funciones y las Cámaras disueltas. Esperar a la constitución de las nuevas Cortes y tramitar un proyecto de ley habría impedido contar con la suficiente celeridad con un marco jurídico preventivo que sirva para proteger los derechos y libertades constitucionalmente reconocidos» (DSCD esmentat, p. 14). L'única justificació que s'aporta, doncs, és que mancaria la «celeritat suficient» per a l'adopció de les mesures, però se segueixen sense exposar els fets concrets que les justificarien ni tampoc no es descriuen els efectes que fan necessària una reacció immediata i no solament preventiva.

A més a més, continuant amb el debat de convalidació, en la resposta de la ministra als representants dels grups parlamentaris, aquesta sosté que «está claro que se trata de una realidad que cambia de forma vertiginosa. Por eso estoy convencida de que tendremos ocasión de trabajar conjuntamente para seguir desarrollando el marco normativo en el ámbito digital en la próxima legislatura, y tener así en cuenta algunas de las propuestas que se han hecho hoy aquí» (DSCD esmentat, p. 31). D'això anterior es desprèn la voluntat que les mesures incorporades al Reial decret llei es tornin a presentar i debatre al llarg de la legislatura següent, perquè la XIII legislatura està a punt de finalitzar. La finalitat de replantejar el contingut de la norma podria posar en qüestió el seu caràcter urgent, ja que hi ha una intenció manifesta d'incorporar les propostes dels grups en una o altres normes, que hauran de ser noves, atès que el dit Reial decret llei no s'ha sotmès a la tramitació com a projecte de llei per convertir-se en llei (art. 86.3 CE).

En conseqüència, manca l'argumentació del per què és indispensable recórrer al decret llei per tal de trobar a temps una solució que no es podria assolir amb el procediment legislatiu ordinari, tant en general com en particular per als preceptes objecte de dictamen.

Per acabar amb la nostra argumentació, i tal com vàrem sostenir en el DCGE 15/2014 (FJ 2), si bé doctrinalment, a l'efecte del seu examen, el caràcter imprevisible o extraordinari de la necessitat és tractat separadament de la urgència, des d'un punt de vista fàctic comparteixen les circumstàncies i motivacions que duen a valorar la situació com a extraordinària, en un cas, i urgent, pel que fa a la via legislativa descartada. Per tant, la manca de concreció de la situació o les situacions a les quals pretenen fer front les mesures previstes en el decret llei i la justificació inexistent del seu caràcter

extraordinari fan alhora impossible determinar perquè no es pot atendre a la via legislativa ordinària.

Consegüentment, estem en condicions d'afirmar que no queda acreditada ni justificada suficientment l'existència d'una necessitat urgent de dictar el Reial decret llei objecte de dictamen en el seu conjunt i dels seus preceptes en concret.

Exposat això anterior resulta innecessari detenir-nos en altres elements qualificadors de la urgència, com ara, l'examen del caràcter immediat dels efectes o l'instantani de les mesures adoptades, com es posa en relleu a la jurisprudència constitucional (STC 332/2005, de 15 de desembre, FJ 7, i STC 96/2014, de 12 de juny, FJ 7); és a dir, fins a quin punt les mesures incorporades al decret llei modifiquen 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).

C) Per concloure amb l'anàlisi del pressupòsit formal habilitant, hem de referir-nos a l'exigència de la connexió de sentit, o la congruència entre les mesures adoptades per la disposició i la finalitat que persegueix. El DCGE 6/2012, FJ 2, ho sintetitza de manera que s'ha d'identificar com l'existència d'un vincle raonable entre les dites mesures i la situació que exigeix l'acció normativa (en aquest sentit, STC 1/2012, FJ 6, 7 i 11), per la qual cosa s'hauran de rebutjar aquelles que «por su contenido y de manera evidente, no guarden relación alguna, directa ni indirecta, con la situación que se trata de afrontar» (STC 1/2012, FJ 11).

La mesura establerta ha de mantenir «la necesaria conexión entre la facultad legislativa excepcional y la existencia del presupuesto [de hecho] habilitante» (STC 68/2007, FJ 6), regla que obliga que el contingut específic d'allò que substantivament prescriu la disposició aprovada respongui a la situació

d'extraordinària i urgent necessitat. És imprescindible examinar el contingut i l'estructura de la disposició normativa aprovada pel Govern (DCGE 16/2013, FJ 3.4) per escatir si hi ha congruència entre la necessitat de dictar-lo i les mesures que l'integren.

En el nostre cas, en no haver-se especificat quina és la situació extraordinària que es vol afrontar, i que fa necessària l'emissió d'un decret llei, difícilment es pot vincular aquesta indeterminació amb les mesures que el Reial decret llei adopta, de forma que es desacredita la connexió de sentit respecte de tot el seu contingut, qüestió que com hem dit abans, constitueix un requisit exigit per la jurisprudència constitucional. A més, ja hem mencionat que les mesures responen a subàmbits normatius diferents que potser adverteixen de l'existència d'una pluralitat de situacions que es volen redreçar, aspecte que tampoc queda aclarit ni fonamentat pel Govern de l'Estat.

D) Finalment, una vegada hem verificat que la definició que el Govern ha fet de la situació de necessitat extraordinària i urgent no ha estat ni explícita ni raonada, i hem constatat la impossibilitat de vincular la situació que es pretén afrontar amb les mesures previstes en la disposició esmentada, estem en condicions d'afirmar que el Govern de l'Estat no ha justificat l'acompliment del requisit formal del pressupòsit habilitant que legitima la validesa constitucional de l'ús del decret llei *ex* article 86.1 CE, i, en conseqüència, el RDL 14/2019 vulnera aquest precepte constitucional.

2. Seguidament, tractarem dels límits del decret llei per raó de l'objecte regulat. Sobre això hem de dir que l'àmbit material vedat a aquestes disposicions ha estat analitzat per la jurisprudència constitucional i per aquest Consell. En particular, ens servirà de referència tant la primerenca STC 111/1983, de 2 de desembre (FJ 8), com la doctrina desenvolupada en resolucions posteriors, com ara les STC 182/1997, de 28 d'octubre (FJ 6 i 7),

i 329/2005 (FJ 8). Pel que fa al Consell, resumirem els DCGE 2/2019, de 22 de febrer (FJ 2.3); 5/2015 (FJ 2.4), i 5/2012 (FJ 2.2).

L'article 86.1 CE fixa els límits materials a què necessàriament s'haurà d'atenir el Govern quan dicti un decret llei, entre els quals, als nostres efectes, no podrà afectar els drets, els deures i les llibertats dels ciutadans regulats en el títol I.

La jurisprudència constitucional ha interpretat que la figura del decret llei no ha de ser entesa de manera tan restrictiva que n'impedeixi l'ús com a instrument normatiu idoni per regular i donar resposta a circumstàncies canviants de la nostra societat (STC 329/2005, FJ 8). Una interpretació estricta i expansiva d'aquesta limitació material continguda a l'article 86.1 CE el buidaria de contingut i el faria inservible per regular, amb més o menys incidència, qualsevol aspecte del títol I de la Constitució (STC 111/1983, FJ 8; 329/2005, FJ 8). En definitiva, si s'interpreta que l'expressió «no podran afectar» concerneix qualsevol regulació que incideixi en els drets constitucionals regulats en el títol I, «el decret llei, com a instrument normatiu previst a la Constitució i a l'Estatut, esdevindria pràcticament inoperant» (DCGE 2/2019, FJ 2.3).

De conformitat amb la jurisprudència constitucional esmentada, no tota regulació que afecti un dret reconegut al títol I de la Constitució està prohibida materialment a la figura del decret llei. Seguint aquesta interpretació, aquesta norma no pot regular, en cap cas, el règim general del dret ni tampoc els seus elements essencials (STC 111/1983, FJ 8, i 182/1997, FJ 6 i 7).

Així, d'acord amb el DCGE 5/2015, quan un decret llei afecti els precitats drets «haurà de respectar el límit infranquejable dels elements essencials del seu règim general, sense alterar-lo ni modificar-lo de manera que no s'innovi

en la configuració que el fa recognoscible com a tal. La modulació i la concreció de l'abast i el rigor de l'acotament […] també variarà, ha recordat el Tribunal Constitucional, segons la naturalesa i, fins i tot, la ubicació sistemàtica del dret en el text constitucional, dins de les diverses seccions i els capítols del títol I» (FJ 2.4).

En tot cas, com vam dir en el DCGE 5/2012, s'ha de subratllar que la doctrina constitucional ha estat essencialment concebuda per evitar la inaplicació de fet de la figura del decret llei, que es derivaria d'una interpretació literal i, per tant, molt estricta, del concepte «afectar» que la Constitució va incorporar, de forma que:

> «A partir d'aquí, podem fixar dos criteris bàsics que cal retenir a fi de determinar l'abast de l'esmentada clàusula restrictiva sobre el decret llei i que es concreten en dos aspectes: d'una banda, que la legislació d'urgència no reguli el règim general dels drets, els deures i les llibertats del títol I CE i que la interpretació constitucionalment adequada tingui en compte la configuració constitucional dels drets en qüestió, la seva ubicació sistemàtica en el títol I CE; i, de l'altra, el major o menor grau d'intensitat o rigor de les garanties de les quals gaudeixen, en virtut del que estableix l'article 53 CE.» (FJ 2.2)

D'aquesta manera, s'afirma en el precitat Dictamen i fonament que «entenem que el "règim general" d'un dret, d'un deure o d'una llibertat és equiparable a l'establiment del seu règim jurídic, és a dir, a l'ordenació de les regles relatives a la titularitat, a l'objecte, a la forma o al procediment que defineixen el dret, a més de les referides als límits i a les garanties per al seu exercici, tots ells elements essencials del dret» (DCGE 5/2012, FJ 2.2).

Així doncs, ens pertoca examinar si els preceptes sol·licitats del Reial decret llei «afecten» en el sentit de l'article 86.1 CE alguns drets fonamentals.

D'entrada, podem descartar una sèrie de preceptes perquè no tenen cap relació, ni tan sols indirecta, amb els drets fonamentals, com ara la regulació del DNI, en document físic o electrònic (art. 1 i 2 RDL 14/2019); la dels sistemes d'identificació i signatura electrònica dels interessats davant les administracions públiques (art. 3.u i .dos RDL 14/2019, pel que fa als art. 9.2.*c* i 10.2.*c* LPACAP); la coordinació en matèria de seguretat de les xarxes (art. 7); les xarxes de comunicacions electròniques en règim d'autoprestació (disp. add. única) i els títols competencials invocats per l'Estat per dictar la norma (disp. final primera), el contingut dels quals es tractarà en els fonaments jurídics següents.

D'altres, com analitzarem posteriorment amb més detall, regulen aspectes relacionats amb el dret a la protecció de dades de caràcter personal (art. 18.4 CE), per tal com incideixen sobre la figura de les transferències internacionals de dades personals, quant a la ubicació territorial dels recursos per al seu tractament i la gestió de determinats sistemes d'identificació i signatura electrònica en el procediment administratiu (art. 3.u i dos RDL 14/2019, pel que fa als articles 9.3 i 10.3 LPACAP) o per a la gestió de determinats sistemes d'informació i de comunicació de les administracions públiques (art. 4.u RDL 14/2019, respecte del nou article 46 bis LPACAP) i també sobre les comunicacions de dades entre administracions públiques (art. 4. dos RDL 14/2019, quant a l'article 155 LRJSP). Ara bé, podem avançar que els preceptes mencionats, com veurem, no estableixen el règim jurídic d'aquest dret, en la mesura que no ordenen les regles relatives a la titularitat, l'objecte, el conjunt de les facultats que el configuren o defineixen, ni els límits o les garanties per al seu exercici, cosa que s'ha efectuat principalment amb la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

De fet, i en aquest sentit, el mateix preàmbul del Reial decret llei declara que aquesta norma es limita a regular «aspectes merament puntuals respecte del

tractament de dades personals per part de les administracions públiques i els seus contractistes a l'empara de l'habilitació que contenen el Reglament UE 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016 i la Llei orgànica 3/2018» (apt. IV, par. segon).

L'argumentació anterior, en relació amb els articles 3 i 4 del Reial decret llei, es pot fer extensiva a les disposicions transitòries primera i segona per tal com fixen el règim transitori de les modificacions d'aquests preceptes.

Pel que fa als preceptes relacionats amb les mesures per reforçar la seguretat en matèria de telecomunicacions, bàsicament l'article 6 del Reial decret llei, en principi tampoc no haurien de constituir una real afectació dels drets fonamentals. Tanmateix, per la tècnica legislativa emprada, l'apartat u i el cinc de l'article 6 RDL 14/2019, en la regulació que fan de la intervenció de les xarxes i els serveis de comunicacions electròniques i del cessament d'una presumpta activitat infractora, prèviament a l'inici del procediment sancionador, respectivament, poden tenir una certa repercussió sobre alguns drets fonamentals i seran examinats després, motiu pel qual ens hem de remetre a les consideracions que realitzarem en el fonament jurídic quart. Com es veurà posteriorment, la seva anàlisi es vincula a la seva qualitat normativa, susceptible d'afectar drets fonamentals (art. 18 i 24 CE) però sense que, en cap cas, tinguin per objecte regular els elements nuclears del seu règim jurídic, inclosos entre els límits materials de la figura del decret llei.

Així doncs, de la lectura de les disposicions sol·licitades, i atesa la regulació material de caràcter sectorial i puntual que duen a terme, es desprèn que cap d'elles pretén una regulació del règim general dels drets mencionats, ni en desenvolupa el seu contingut essencial, entès com les facultats o possibilitats d'actuació que els fan recognoscibles, ni comporta unes limitacions substancials que els facin impracticables.

Això anterior, com hem advertit, sens perjudici de les precisions que farem en els fonaments jurídics següents sobre el contingut i l'abast dels concrets preceptes qüestionats i, quan escaigui, sobre la vulneració o no dels drets suara esmentats.

En conseqüència, en aplicació de la doctrina constitucional i consultiva que acabem d'exposar, estem en condicions de dir que els preceptes sol·licitats del Reial decret llei 14/2019, en no afectar el règim o els elements essencials dels drets, no vulneren els límits materials que exigeix l'article 86.1 CE.

A tall de conclusió del que hem exposat en aquest fonament jurídic, entenem que el Reial decret llei 14/2019 i, en concret, els articles 1, 2, 3, 4, 6, 7, les disposicions addicional única i transitòries primera i segona i la disposició final primera són contraris a l'article 86.1 CE, perquè no compleixen el requisit constitucional de l'extraordinària i urgent necessitat.

Tercer. L'examen de l'adequació constitucional i estatutària dels preceptes del Reial decret llei 14/2019 relatius al document nacional d'identitat i a la identificació electrònica davant les administracions públiques

En aquest fonament jurídic tractarem primer les mesures introduïdes en matèria de documentació nacional d'identitat (art. 1 i 2 RDL 14/2019 que modifiquen els art. 8.1 LOPSC i 15.1 LSE, respectivament) i segonament ens referirem a les que es relacionen amb la identificació electrònica davant les administracions públiques (art. 3.u i .dos RDL 14/2019, en allò referit als art. 9.2 i 10.2 LPACAP).

Es tracta d'àmbits regulatoris diferents, relatius a l'acreditació de la identitat d'una persona física i als sistemes d'identificació electrònica validats per als interessats (ja siguin persona física o jurídica) en la seva relació amb les administracions públiques. Com veurem a continuació, les particularitats i el context normatiu del document nacional d'identitat (en endavant, DNI), d'una banda, i els dels sistemes d'identificació esmentats, de l'altra, ens ubiquen en matèries competencials diferents, que permeten a l'Estat i a les comunitats autònomes unes facultats normatives i executives distintes. Tanmateix, el paper que el primer pot representar també com a sistema d'identificació dels interessats davant les administracions públiques justifica que ho tractem en aquest mateix fonament jurídic.

1. Per tal de donar adequada resposta als dubtes de naturalesa competencial que la sol·licitud planteja en relació amb el primer bloc de preceptes qüestionats, sobre les mesures en matèria de documentació nacional d'identitat, haurem d'enquadrar materialment les normes qüestionades, a fi de determinar el títol prevalent en què s'empara i el seu abast, cosa que farem tenint en compte la descripció del contingut i la finalitat dels preceptes sol·licitats, la petició del Govern, la naturalesa i les funcions del DNI, així com els precedents i el context normatiu dels dits preceptes.

A) Resumidament, els articles 1 i 2 RDL 14/2019 modifiquen l'article 8.1 LOPSC i l'article 15.1 LSE, que, respectivament, regulen la naturalesa i els efectes del DNI, en format físic i electrònic, en el sentit següent. D'una banda, l'article 8.1 diu que els espanyols tenen dret a l'expedició del seu DNI i que aquest és un document públic i oficial. A més, com a relativa novetat, ho declara amb més èmfasi, en prescriure que és «l'únic document» amb suficient valor per si mateix per a l'acreditació, «a tots els efectes», de la identitat i de les dades personals del seu titular. D'altra banda, l'article 15.1 LSE diu que el DNI electrònic acredita la identitat personal del seu titular, en aquest cas electrònicament, i permet la signatura electrònica de documents,

establint, com a novetat, una remissió als termes en què l'article 8.1 LOPSC disposa que el DNI acredita la dita identitat personal.

La disposició final primera, apartat 1, del Reial decret llei que estem dictaminant estableix que els articles 1 i 2 es dicten a l'empara de l'article 149.1.29 CE, que atribueix a l'Estat la competència exclusiva en matèria de seguretat pública. La sol·licitud del Govern no nega que la matèria regulada pels esmentats preceptes s'ubiqui en l'al·ludit títol competencial de seguretat pública (art. 149.1.29 CE), sinó que centra el seu qüestionament en el possible efecte restrictiu que la concreta regulació que ara es fa pot tenir sobre les competències de la Generalitat per determinar els sistemes d'identificació dels interessats davant les administracions públiques, incidint en les competències previstes als articles 150 i 159 EAC. En concret, critica que la principal conseqüència d'aquesta modificació és que la creació de sistemes d'identificació i signatura haurà d'anar precedida d'una identificació personal que només podrà realitzar-se a través del DNI.

Sobre això, hem de començar recordant que el DNI, que s'expedeix a tots els espanyols, esdevé una conseqüència de la nacionalitat, de manera que tots els ciutadans espanyols tenen dret a disposar-ne (art. 8.1 LOPSC). Aquesta relació amb la nacionalitat, tanmateix, és només indirecta i no implica cap mena d'encavallament amb l'article 149.1.2 CE que, d'altra banda, també atribueix en exclusiva a l'Estat la competència per regular aquest àmbit material, com veurem en descriure el cànon competencial.

El dret dels ciutadans espanyols que l'Estat els expedeixi el DNI es relaciona amb el dret a la identitat o al reconeixement de la personalitat jurídica previst a l'article 6 de la Declaració universal de drets de l'home i a l'article 16 del Pacte internacional de drets civils i polítics; relació que deriva del fet que l'esmentat document públic és el mitjà ordinari d'acreditació de dita personalitat jurídica. Cal tenir en compte que la identitat d'una persona

física, com a dret, no només fa referència als trets i les dades personals que la caracteritzen i la individualitzen, sinó també al dret a conèixer els propis orígens i a la identitat sexual, entre d'altres, però aquests darrers aspectes, òbviament, resten fora de la identitat més bàsica a què es refereix el DNI i, per tant, han de quedar al marge de l'objecte del present Dictamen. Aquí tan sols ens limitarem a destacar que la importància d'aquest dret l'ha posat en relleu, darrerament, la recent STC 99/2019, de 18 de juliol, assenyalant que «si bien este derecho no se reconoce como tal en la Constitución Española de 1978, se puede considerar tácitamente incluido en el art. 10.1 CE, aparte de que sí está reconocido tanto en el art. 8 de la Convención sobre los derechos del niño de 2006 como en la Carta europea de los derechos del niño de 1992» (FJ 8).

Pel que interessa als efectes d'aquest Dictamen, cal tenir present, igualment, que l'acreditació de la identitat dels ciutadans és la premissa determinant i imprescindible per tal que els poders públics puguin complir la seva funció de persecució dels delictes i garantir també la seguretat ciutadana i la pau social. És en aquest àmbit material de la seguretat pública (art. 149.1.29 CE) on, precisament, se situen les mesures que atribueixen al DNI caràcter exclusiu i excloent, com a únic document amb suficient valor per si sol per a l'acreditació, a tots els efectes, de la identitat i les dades personals del seu titular. De fet, garantir el compliment dels fins que persegueix la llei de seguretat ciutadana és el sentit al qual respon tota aquesta regulació sobre la documentació i identificació dels ciutadans espanyols, el valor probatori del document nacional d'identitat i el passaport, així com els deures dels seus titulars, i la incorporació de les possibilitats d'acreditació electrònica de la identitat i el manteniment de l'exigència d'exhibir-los a requeriment dels agents de l'autoritat en els supòsits i amb les garanties que preveu la llei (art. 9.2 i 16 LOPSC), tal com resulta dels apartats II i III del preàmbul de la LOPSC i ha afirmat també la STC 25/2004, de 26 de febrer (FJ 6).

L'article 9.1 LOPSC, per les mateixes raons de seguretat pública, remarca igualment la rellevància d'aquest document d'identificació establint que cap espanyol pot ser privat del DNI, ni tan sols temporalment, llevat dels casos i la forma establerts per les lleis en què hagi de ser substituït per un altre document.

I tot això és així prescindint, fins i tot, del fet que, tradicionalment, la competència per expedir el DNI s'hagi atribuït a l'autoritat policial, concretament al Ministeri de l'Interior (a través de la Direcció General de Policia) a la qual, a més, correspon la custòdia i responsabilitat dels arxius i fitxers que s'hi relacionen; competència orgànica prevista per l'article 10 LOPSC (que l'art. 12.1.A.*a* de la Llei orgànica 2/1986, de 13 de març, de forces i cossos de seguretat assigna més concretament encara al «Cos Nacional de Policia») que, per cert, no deriva de cap mandat constitucional. Dit això, volem destacar, encara que només sigui de passada, que aquesta atribució de la competència per al seu atorgament a organismes responsables de la seguretat ciutadana, no significa que sigui un document que es relacioni exclusivament amb l'àmbit policial i amb la dita seguretat. En efecte, com ja s'ha dit, el DNI és, destacadament, un document acreditatiu de la personalitat jurídica (en expressió de l'art. 6 de la Declaració universal de drets humans de 1948) del seu titular, motiu pel qual potser fóra més escaient que l'esmentada competència orgànica s'atribuís al Registre Civil, però aquesta és una qüestió en què no ens correspon entrar.

La vinculació de la present regulació del DNI a la seguretat pública no exclou, com és obvi, que, com a sistema d'identificació dels ciutadans espanyols, aquest document d'identitat sigui igualment essencial en altres àmbits aliens a la seguretat pública, com pot ser, per exemple, el fiscal, a l'hora de permetre que l'Administració tributària dugui a terme les corresponents activitats de control. En aquest sentit, a banda del fet que el DNI sigui referent obligat per a l'expedició d'altres documents d'especial rellevància

com són el passaport o la identificació fiscal, i de les funcions específiques que la normativa sobre seguretat ciutadana ha atribuït al DNI, cal fer notar que en diversos sectors de l'ordenament jurídic podem trobar exemples d'altres mitjans admesos per a la identificació dels ciutadans espanyols.

A títol il·lustratiu, cal fer esment de la possibilitat d'identificar els electors per part de la mesa electoral també mitjançant el passaport o el permís de conduir en què aparegui la fotografia del titular (art. 85 Llei orgànica 5/1985, de 19 de juny, del règim electoral general); l'acreditació de la nacionalitat i la identitat dels atorgants o compareixents espanyols en una escriptura pública mitjançant DNI o passaport (art. 161 Reglament de l'organització i el règim del notariat, aprovat pel Decret de 2 de juny de 1944, modificat pel Reial decret 45/2007, de 19 de gener), o la identificació de les persones que es facin càrrec d'enviaments postals davant l'operador postal que realitzi l'entrega mitjançant l'exhibició del DNI, passaport o permís de conduir (art. 32.1 Reial decret 1829/1999, de 3 de desembre, pel qual s'aprova el Reglament pel qual es regula la prestació dels serveis postals, en desenvolupament de la Llei 24/1998, de 13 de juliol, del servei postal universal i de liberalització dels serveis postals).

Un cop hem descrit la naturalesa i les principals funcions del DNI, especialment pel que fa a l'àmbit de la seguretat ciutadana, tot seguit, abans de procedir a l'enquadrament competencial definitiu dels preceptes qüestionats, formularem algunes consideracions generals sobre els precedents i el context que delimiten la legislació i el marc regulador del DNI.

Els precedents de la LOPSC els trobem, primerament, al Decret 196/1976, de 6 de febrer, pel qual es regula el document nacional d'identitat que, pel que aquí interessa, el configurava com «un documento público que acredita la auténtica personalidad de su titular, constituyendo el único y exclusivo justificante completo de la identificación de la persona. Será imprescindible

para justificar por sí mismo y oficialmente la personalidad de su titular, haciendo fe, salvo prueba en contrario, de los datos personales que en él se consignen». I, més endavant, a la Llei orgànica 1/1992, de 21 de febrer, sobre protecció de la seguretat ciutadana, dictada també a l'empara de la competència estatal de l'article 149.1.29 CE sobre seguretat pública, que ja establia el dret i el deure d'obtenir el DNI a partir dels 14 anys, el qual tenia per si sol suficient valor per acreditar la identitat dels ciutadans espanyols; l'expedició del passaport o document equivalent, i el deure d'identificació dels estrangers que es trobessin a Espanya (cap. II, secció III), així com les condicions en què les forces i els cossos de seguretat podien requerir la identificació de les persones (cap. III).

L'actual normació del DNI es troba, principalment, en la LOPSC; la Llei 84/1978, de 28 de desembre, per la qual es regula la seva taxa d'expedició; la LSE, quant al DNI electrònic, i el Reial decret 1553/2005, de 23 de desembre, pel qual es regula l'expedició del document nacional d'identitat i els seus certificats de signatura electrònica.

Concretament, el capítol II de la LOPSC, intitulat «Documentació i identificació personal» (art. 8 a 13) i dictat a l'empara de l'article 149.1.29 CE, determina el valor probatori del DNI i del passaport i els deures dels titulars d'aquests documents, incorpora les possibilitats d'identificació i de signatura electrònica i n'exigeix l'exhibició a requeriment dels agents de l'autoritat, d'acord amb el que preveu la Llei (art. 16, entre d'altres). Pel que fa al passaport, la mateixa LOPSC el configura com a document públic, personal, individual i intransferible que, llevat que hi hagi una prova en contra, acredita la identitat i la nacionalitat dels ciutadans espanyols fora d'Espanya i, dins del territori nacional, les mateixes circumstàncies dels espanyols no residents (art. 11 LOPSC). D'això resulta que ambdós documents acrediten, amb caràcter general i en els termes exposats, la

identitat dels espanyols, per bé que el DNI és l'únic que, en tot cas, té suficient valor identificatiu per si sol.

En l'entorn digital, el DNI electrònic, en el cas dels espanyols majors d'edat que gaudeixin de plena capacitat d'obrar i dels menors emancipats, a més d'acreditar la identitat en el sentit tradicional, permet la identificació electrònica del seu titular i la signatura electrònica de documents, en els termes previstos a la legislació específica (art. 8.3 LOPSC i art. 15.1 LSE), atès que incorpora el certificat i la signatura electrònics. En aquest punt, la LSE es limita a fixar el seu marc normatiu bàsic establint el deure de totes les persones físiques o jurídiques, públiques o privades, de reconèixer l'eficàcia del document nacional d'identitat electrònic per verificar la identitat i les altres dades personals del titular que hi constin, i per acreditar la identitat del signant i la integritat dels documents signats amb els dispositius de signatura electrònica que hi estan inclosos (art. 15.2 LSE). En desenvolupament de la Llei orgànica 1/1992 i de la regulació continguda en la LSE i el mandat recollit en la seva disposició final segona, es va aprovar l'abans esmentat RD 1553/2005, al qual ja hem fet referència.

Així mateix, pel que fa a la identificació dels interessats en el procediment administratiu, l'article 9.1 de la LPACAP obliga les administracions a verificar la identitat dels interessats «mitjançant la comprovació del seu nom i cognoms o denominació o raó social, segons que correspongui, que constin al document nacional d'identitat o document identificatiu equivalent». Quant a la seva identificació electrònica, ens remetem a l'anàlisi de l'article 3.u i .dos RDL 14/2019 que realitzarem més endavant en aquest mateix fonament jurídic.

B) Fetes les anteriors precisions, passarem a exposar el paràmetre de constitucionalitat relatiu a les competències de l'Estat en matèria de

seguretat pública (art. 149.1.29 CE), que és on hem determinat que s'enquadren competencialment els articles sol·licitats.

Hem de començar, per tant, per definir de forma breu quin és el seu significat, ja que l'haurem de tornar a tractar altres vegades en aquest Dictamen, relacionant-lo amb altres títols que incideixen en altres preceptes sol·licitats (com ara, defensa a l'art. 149.1.4 CE, bases del règim jurídic de les administracions públiques i procediment administratiu comú, a l'art. 149.1.18 CE, o règim general de les comunicacions, a l'art. 149.1.21 CE).

La competència sobre seguretat pública ha estat tractada en diverses ocasions per aquest Consell (DCGE 18/2015, de 26 de novembre, FJ 2) i per la jurisprudència constitucional (per totes, STC 25/2004, de 26 de febrer, FJ 6), que resumirem més endavant.

D'acord amb l'article 149.1.29 CE, es tracta d'una competència assignada constitucionalment i principal a l'Estat, si bé ha de desplegar-se sense perjudici de la creació de policies per part de les comunitats autònomes. On aquestes existeixin hi haurà una certa concurrència competencial, per mandat constitucional, en el marc d'una llei orgànica de repartiment funcional. Aquesta Llei orgànica és la 2/1986, de 13 de març, de forces i cossos de seguretat de l'Estat. L'article 13 de l'Estatut d'autonomia de 1979 (i ara el 164 EAC) va permetre assumir competències en seguretat i crear els Mossos d'Esquadra com a cos policial de Catalunya.

El DNI s'expedeix a tots els espanyols, constitueix ensems una conseqüència de la nacionalitat, de manera que tots els espanyols hi tenen dret (art. 8.1 LOPSC), sense que això vulgui dir, però, que afecti el títol competencial de l'article 149.1.2 CE. En efecte, sobre l'abast material de la regulació de la nacionalitat podem recórrer a la Declaració 1/1992 del Tribunal Constitucional, d'1 de juliol, segons la qual:

> «El legislador de la nacionalidad debe, como es obvio, definir quiénes son españoles, es decir, quiénes tienen, potencialmente, capacidad para ser titulares de cualesquiera situaciones jurídicas en el ordenamiento y sobre ello no le da la Constitución pauta material alguna. Pero no puede, sin incurrir en inconstitucionalidad, fragmentar, parcelar o manipular esa condición, reconociéndola solamente a determinados efectos con el único objeto de conceder a quienes no son nacionales un derecho fundamental.» (FJ 5)

És a dir, la regulació de l'Estat sobre la nacionalitat i els seus efectes comporta donar el dret a obtenir el DNI als nacionals, com a document identificador. La regulació del DNI, en tant que conseqüència de la nacionalitat, no constitueix una ordenació d'aquesta (art. 149.1.2 CE), ja que no determina qui és i qui no és nacional, ni estableix els requisits necessaris per adquirir la nacionalitat, sinó que prescriu un dels seus efectes: permetre acreditar que es disposa de la nacionalitat espanyola, de manera que, com hem dit a l'inici d'aquest fonament jurídic, la competència en matèria de nacionalitat no desplaça la seguretat pública com a prevalent en el supòsit que ara s'examina.

Així, per completar el paràmetre de constitucionalitat i d'estatutarietat que ha de guiar el nostre pronunciament sobre els esmentats articles 1 i 2 RDL 14/2019, ens referirem molt breument a la jurisprudència constitucional. La STC 104/1989, de 8 de juny, afirma que la seguretat pública es refereix a la «protección de personas y bienes y al mantenimiento de la tranquilidad u orden ciudadano» (FJ 3). A la STC 25/2004, el Tribunal Constitucional ho precisa dient que la dita matèria inclou «un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido» i situa al si del títol, de forma predominant, «las organizaciones y los medios instrumentales, en especial los cuerpos de seguridad a que se refiere el art. 104 CE» (FJ 6).

Tanmateix, també ha ampliat el concepte de seguretat pública més enllà de la regulació de les intervencions de la policia de seguretat (STC 148/2000, de 1 de juny, FJ 6). En aquest sentit, hi afegeix «[o]tros aspectos y otras funciones distintas de los cuerpos y fuerzas de seguridad, y atribuidas a otros órganos y autoridades administrativas» (STC 104/1989, de 8 de juny, FJ 3). D'aquesta manera, com hem enunciat en tractar de l'enquadrament competencial d'ambdós preceptes qüestionats, la STC 25/2004, referint-se a l'ara derogada LO 1/1992, inclou, entre els àmbits als quals es constreny la regulació que fa la dita llei, l'establiment de la responsabilitat de les autoritats en allò que es refereix a la documentació personal de nacionals i estrangers a Espanya, entenent que són aspectes susceptibles «de originar riesgos ciertos que pueden afectar de modo directo y grave a la seguridad de personas y bienes» (FJ 6), sense la voluntat d'estendre la regulació a qualsevol activitat que tingui una relació més o menys estreta amb la seguretat pública.

C) Un cop ha quedat concretat el paràmetre competencial aplicable al nucli principal de la matèria que regula el Reial decret llei en relació amb el DNI, ens correspon examinar ara si els preceptes qüestionats s'hi ajusten o, el que és el mateix, si, tal com denuncia la sol·licitud, comporten una restricció o un desplaçament de les competències de la Generalitat per determinar els sistemes d'identificació dels interessats davant de les administracions públiques en el si del procediment administratiu regulat a la LPACAP (art. 150 i 159 EAC). I, de manera més concreta, si la principal conseqüència d'aquesta previsió és que «inexcusablement, la creació de sistemes d'identificació i signatura haurà d'anar precedida d'una identificació personal que només podrà acreditar-se mitjançant DNI».

Per a una millor comprensió de la seva anàlisi, que realitzarem de forma conjunta atesa la connexió indestriable que hi ha entre ambdós articles, els reproduirem tot seguit en la seva literalitat.

L'article 1 RDL 14/2019 modifica l'apartat 1 de l'article 8 LOPSC el qual queda redactat amb el contingut següent:

> «1. Els espanyols tenen dret que se'ls expedeixi el document nacional d'identitat.
> El document nacional d'identitat és un document públic i oficial i té la protecció que a aquests tipus de documents atorguen les lleis. És l'únic document amb prou valor per si sol per acreditar, a tots els efectes, la identitat i les dades personals del seu titular.»

Per la seva banda, l'article 2 RDL 14/2019 modifica l'apartat 1 de l'article 15 LSE en els termes següents:

> «1. El document nacional d'identitat electrònic és el document nacional d'identitat que acredita electrònicament la identitat personal del titular, en els termes que estableix l'article 8 de la Llei orgànica 4/2015, de 30 de març, de protecció de la seguretat ciutadana, i permet la signatura electrònica de documents.»

Tal com ha quedat dit al començament d'aquest fonament jurídic, la modificació introduïda a l'article 8.1 LOPSC consisteix a afegir que el DNI és «l'únic document» amb suficient valor per si sol per acreditar «a tots els efectes» la identitat del titular i les seves dades personals. I, pel que fa a l'article 15.1 LSE, la reforma es limita a incorporar una remissió a l'esmentat article 8.1 LOPSC.

Hem de començar recordant, novament, que amb l'atribució al DNI, amb caràcter d'únic i exclusiu, de la condició de justificant complet de l'autèntica personalitat del seu titular, es recupera una característica que, segons hem exposat en aquest mateix fonament jurídic, en tractar de la naturalesa

d'aquest document identificatiu, ja li atribuïa l'article 1 del Decret 196/1976, de 6 de febrer, que aleshores regulava el document nacional d'identitat.

A partir d'aquí, entenem que el sentit que s'ha de donar al restabliment d'aquesta exclusivitat és que cap autoritat ni tampoc cap particular poden exigir en l'àmbit de la seguretat pública un document diferent al DNI per acreditar la identitat i les dades personals dels seus titulars. Hem de recordar, novament, que es tracta de normes que se situen en l'àmbit material de la seguretat pública, on la identitat de les persones constitueix la premissa determinant i imprescindible per tal que els poders públics puguin desenvolupar la seva funció de garantir la dita seguretat i la pau social.

Per aquesta raó i quan es tracti d'altres situacions, res no exclou que les administracions públiques, per a l'exercici de determinats drets o el gaudi de prestacions públiques, puguin exigir, d'acord amb les seves competències, que els ciutadans espanyols hagin d'estar en possessió d'algun altre document acreditatiu o que en el procediment administratiu es puguin identificar electrònicament també a través de sistemes diferents del DNI.

En aquest sentit, la primera conseqüència que, amb caràcter general, es pot extreure de l'article 15.1 LSE és que els titulars del DNI electrònic són alhora titulars d'una signatura electrònica reconeguda, sens perjudici dels altres sistemes d'identificació que es preveuen en aquest mateix article. A banda de l'anterior, cal tenir present, també, que la signatura i el certificat electrònics continguts en el DNI electrònic són de caràcter més reforçat que la resta de signatures electròniques reconegudes, ja que tothom, incloses les diferents administracions públiques, l'ha de reconèixer en el seu doble vessant: com a identificador del seu titular i com a signatura de documents electrònics (art. 15.2 LSE).

Ara bé, la remissió de l'article 15.1 LSE al fet que l'acreditació electrònica de la identitat personal del titular del DNI ho és «en els termes que estableix l'article 8 de la Llei orgànica 4/2015, de 30 de març, de protecció de la seguretat ciutadana» no implica que els sistemes d'identificació i signatura hagin d'anar precedits d'una identificació personal que només pugui acreditar-se mitjançant DNI.

Aquesta constatació es confirma amb el fet que la modificació realitzada pels articles 1 i 2 RDL 14/2019 s'ha produït sense canviar la normativa bàsica estatal, llevat el que després direm sobre l'autorització estatal prèvia, en el cas dels sistemes de clau concertada i altres sistemes equiparats. És a dir, d'una banda, s'ha mantingut la regla segons la qual les administracions públiques poden verificar la identitat dels interessats en el procediment administratiu, mitjançant la comprovació del seu nom i cognoms que constin en el DNI o en un document identificatiu equivalent (art. 9.1 LPACAP), i, de l'altra, es manté igualment la possibilitat que els interessats s'identifiquin davant les administracions públiques a través de sistemes basats en certificats electrònics, de clau concertada o de qualsevol altre sistema que les administracions considerin vàlid (com ara l'idCAT Mòbil o el SIVCat), en els termes i les condicions que s'estableixi (art. 9.2 LPACAP), sense cap altre requisit.

Les consideracions efectuades ens porten a afirmar que la determinació del DNI com a «únic document» amb suficient valor per si sol per a l'acreditació «a tots els efectes» de la identitat i dades personals del seu titular només impedeix que se'n pugui crear un altre d'equivalent amb la mateixa consideració i eficàcia que descriu l'article 8.1 LOPSC. Per tant, la reforma no introdueix cap debilitació respecte de la validesa d'altres sistemes d'identificació i signatura a través d'altres documents identificatius com podria ser, per exemple, la targeta d'identificació sanitària de la Generalitat. Dit amb unes altres paraules, la modificació d'ambdós preceptes se

circumscriu a l'acreditació de la identitat i les dades personals en l'àmbit de la seguretat pública i no implica que en tots els procediments administratius calgui sempre aportar el DNI com a element addicional d'acreditació.

Així, doncs, a diferència del que se sosté en la sol·licitud, entenem que establir que el DNI sigui l'únic document amb valor suficient per acreditar, per si sol, la identitat i les dades personals del seu titular, en res afecta la competència de la Generalitat de Catalunya per organitzar la seva pròpia Administració (art. 150 EAC), ni tampoc la que li correspon en matèria de règim jurídic i procediment de les administracions públiques catalanes (art. 159 EAC).

En conseqüència, els articles 1 i 2 RDL 14/2019, de 31 d'octubre, en la modificació que fan, respectivament, de l'apartat 1 de l'article 8 de la Llei orgànica 4/2015, de 30 de març, de protecció de la seguretat ciutadana, i de l'apartat 1 de l'article 15 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, es dicten d'acord amb l'article 149.1.29 CE i no vulneren les competències de la Generalitat assumides pels articles 150 i 159 EAC.

2. A continuació, analitzarem l'article 3 RDL 14/2019, apartats primer i segon, quant a les modificacions introduïdes en els articles 9.2 i 10.2 LPACAP, preceptes que contenen un conjunt de mesures en matèria d'identificació i signatura electròniques dels interessats en el procediment administratiu. Per la seva vinculació, també examinarem l'apartat 1 de la disposició transitòria primera del Reial decret llei, que estableix el règim transitori de les mesures anteriors.

Atès que els canvis introduïts en les lletres *a* i *b* dels articles 9.2 i 10.2 LPACAP no han estat qüestionats pel sol·licitant i responen, tal com manifesta el preàmbul del Reial decret llei, a la necessitat d'adaptar el seu

contingut al 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 al mercat interior i pel qual es deroga la Directiva 1999/93/CE (en endavant, Reglament eIDAS), limitarem la nostra anàlisi, quant a aquests preceptes, únicament a la nova redacció de la seva lletra *c*.

Iniciarem, doncs, la nostra tasca consultiva amb l'examen de la vigent redacció dels articles 9.2.*c* i 10.2.*c* LPACAP, així com de la disposició transitòria primera.1 RDL 14/2019.

Amb caràcter previ i introductori a l'anàlisi dels preceptes, efectuarem, de forma succinta, diverses consideracions generals sobre el context en què s'insereixen. Posteriorment, realitzarem el seu enquadrament, exposarem breument el paràmetre de constitucionalitat i d'estatutarietat que resulti aplicable i, seguidament, l'aplicarem a les normes qüestionades pel peticionari.

A) La creació d'un clima de confiança en les transaccions electròniques, en el mercat interior de la Unió Europea, per assolir interaccions electròniques segures entre els ciutadans, les empreses i les administracions públiques, ha impulsat l'adopció del Reglament eIDAS, el qual ha estat aprovat en compliment del Pla d'acció europeu d'administració electrònica 2011-2015 i l'Agenda Digital per a Europa. El Reglament té un doble objectiu: garantir el correcte funcionament del mercat interior i, alhora, assolir un nivell de seguretat dels mitjans d'identificació electrònica i els serveis de confiança, i es limita a establir les condicions en què els estats membres han de reconèixer els mitjans d'identificació electrònica notificats a la Comissió per un altre Estat membre, establint un marc jurídic per al reconeixement mutu dels sistemes en qüestió (art. 1).

Aquesta norma europea, d'aplicació directa, regula, entre altres figures, la signatura electrònica (avançada i qualificada) i el segell electrònic (avançat i qualificat). Així, en primer lloc, defineix la signatura electrònica com les dades en format electrònic annexes a altres dades electròniques o associades de manera lògica amb aquestes que utilitza el signant per firmar. En segon lloc, precisa que la signatura electrònica avançada és aquella que està vinculada al signant de manera única, en permet la identificació, ha estat creada utilitzant dades de creació de la signatura electrònica que el signant pot utilitzar amb un alt nivell de confiança sota el seu control exclusiu i està vinculada amb les dades signades de manera que qualsevol modificació posterior d'aquestes sigui detectable (art. 26). Finalment, entén la signatura electrònica qualificada com aquella signatura avançada que es crea mitjançant un dispositiu qualificat de creació de signatures electròniques i que es basa en un certificat qualificat de signatura electrònica (art. 3.12), és a dir, un certificat expedit per un prestador qualificat de serveis de confiança que compleix els requisits establerts en l'annex I de la norma (art. 3.15).

El Reglament diferencia entre signatura electrònica, de persona física, i el segell electrònic, de persona jurídica, admetent també, en aquest cas, la signatura electrònica qualificada del representant autoritzat de la persona jurídica (considerants 58 i 59).

Quant als efectes jurídics, la norma estableix, d'una banda, que no es poden denegar efectes jurídics ni admissibilitat com a prova en procediments judicials a una signatura electrònica o un segell electrònic pel simple fet de ser electrònic o perquè no compleixi els requisits de la signatura o del segell electrònic qualificat (art. 25.1 i 35.1). I, de l'altra, indica que la signatura electrònica qualificada té un efecte jurídic equivalent al de la manuscrita (art. 25.2), mentre que un segell electrònic qualificat gaudirà de la presumpció d'integritat de les dades i de la correcció de l'origen de les dades a les quals el segell estigui vinculat (art. 35.2).

En matèria de signatura electrònica, l'Estat va transposar la Directiva 1999/93/CE, ja citada, mitjançant el Reial decret llei 14/1999, de 17 de setembre, de signatura electrònica. Posteriorment, en haver decaigut la iniciativa legislativa impulsada per a la tramitació d'aquesta norma com a projecte de llei, la va transposar a través de la LSE. Aquesta norma regula la firma electrònica, la seva eficàcia jurídica i la prestació de serveis de certificació. En aquest sentit, la LSE defineix la signatura electrònica en termes similars al Reglament europeu. Distingeix entre la signatura avançada (art. 3.2), que equival a la signatura homònima prevista al Reglament eIDAS, i la reconeguda (art. 3.3), que es correspon amb la signatura electrònica qualificada, i regula els certificats electrònics de persones jurídiques (art. 7).

Igualment, la identificació electrònica ha estat regulada en diverses normes de desenvolupament de la denominada administració electrònica, com ara la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics (actualment derogada, llevat de determinats articles d'acord amb la disposició final setena de la LPACAP). Aquesta Llei 11/2007 va reconèixer el dret dels ciutadans a relacionar-se electrònicament amb les administracions públiques i el deure d'aquestes de dotar-se dels mitjans i sistemes necessaris perquè aquest dret pugui exercir-se, i va regular les formes d'identificació i autenticació admissibles, dret i deure actualment previstos en els articles 9, 12 i 13 LPACAP.

Al respecte, una de les novetats que va introduir la LPACAP és la separació entre identificació i signatura electrònica i la simplificació dels sistemes corresponents. Pel que fa als sistemes d'identificació, després d'establir el deure de verificar la identitat dels interessats en el procediment administratiu, mitjançant DNI o document acreditatiu equivalent, l'article 9 LPACAP, en la seva redacció anterior, exigia, amb caràcter general, un

registre previ com a usuari per acreditar la identitat del titular. A més, admetia els basats en certificats electrònics reconeguts o qualificats de signatura electrònica o de segell electrònic expedits per prestadors autoritzats i els sistemes de clau concertada o qualsevol altre que es considerés vàlid, de manera que corresponia a cada administració determinar si autoritzava tots o alguns dels sistemes i la relació entre el tipus d'identificació i el tràmit o procediment. Ara bé, com a límit a l'admissió de sistemes d'identificació no basats en certificats electrònics, s'establia l'obligació per a l'Administració d'acceptar tots els altres sistemes.

Pel que fa als sistemes de signatura, l'article 10 LPACAP, després d'establir que es pot firmar per qualsevol mitjà que permeti acreditar l'autenticitat de l'expressió de la voluntat i del consentiment, així com la integritat i inalterabilitat del document signat, assenyalava com a vàlids, en la seva redacció immediatament anterior, els sistemes de signatura reconeguda o qualificada i avançada o de segell electrònic reconegut o qualificat i de segell electrònic avançat basats en certificats electrònics reconeguts o qualificats de signatura electrònica o de segell electrònic, expedits per prestadors autoritzats, així com qualsevol altre que les administracions consideressin vàlid. Aquests sistemes han de comptar (com en l'article 9.2.*c* LPACAP) amb un registre previ dels usuaris que permeti garantir la seva identitat.

En el marc de les administracions públiques catalanes, la Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya, reconeix el dret d'obtenir i utilitzar qualsevol sistema de signatura electrònica, en els termes i amb els límits que s'estableixin normativament (art. 24.5). Ultra això, disposa que les persones físiques poden fer servir sempre, en les relacions amb les administracions, els sistemes de signatura electrònica incorporats en el document nacional d'identitat, si bé també poden utilitzar altres sistemes admesos per les administracions (art. 45). Accepta, també, la validesa del sistema

d'identificació, autenticació i signatura electrònica no avançada en l'àmbit de l'Administració de la Generalitat i en les seves relacions amb els ciutadans, les entitats, fundacions i associacions inscrites en els registres públics, les empreses i altres organismes públics. També permet l'ús de claus concertades en un registre previ, la informació coneguda pels ciutadans i per les administracions, i les dades i els codis alfanumèrics que figurin impresos en targetes identificadores o d'accés a serveis públics expedides per les administracions per verificar la identificació i autenticació dels ciutadans i fer el seu registre electrònic sense certificat digital (disp. add. setzena).

En les relacions electròniques amb l'Administració de la Generalitat, les persones físiques poden utilitzar en tot cas els sistemes de signatura electrònica incorporats en el document nacional d'identitat, els certificats idCAT i, talment com les persones jurídiques, els sistemes previstos en el protocol d'identificació i signatura electrònica (art. 29 i 30 Decret 56/2009, de 7 d'abril, per a l'impuls i el desenvolupament dels mitjans electrònics a l'Administració de la Generalitat), aprovat per l'Ordre GRI /233/2015, de 20 de juliol, que recull els aspectes tècnics i organitzatius necessaris per a la implantació dels sistemes de signatura electrònica per a cada tràmit o servei, en funció del grau de seguretat que es requereixi.

Un cop vist el context normatiu en matèria d'identificació i signatura electrònica en les relacions entre els particulars i les administracions, estem en disposició d'analitzar el contingut de les modificacions introduïdes a la LPACAP per part del Reial decret llei en aquests àmbits materials.

L'article 3.u del Reial decret llei modifica l'apartat 2 de l'article 9 LPACAP, sobre els sistemes d'identificació dels interessats en el procediment, que queda redactat amb el contingut següent:

> «2. Els interessats es poden identificar electrònicament davant les administracions públiques a través dels sistemes següents:
> a) Sistemes basats en certificats electrònics qualificats de signatura electrònica expedits per prestadors inclosos a la ‘‘Llista de confiança de prestadors de serveis de certificació’’.
> b) Sistemes basats en certificats electrònics qualificats de segell electrònic expedits per prestadors inclosos a la ‘‘Llista de confiança de prestadors de serveis de certificació’’.
> c) Sistemes de clau concertada i qualsevol altre sistema que les administracions considerin vàlid en els termes i les condicions que s'estableixin, sempre que tinguin un registre previ com a usuari que permeti garantir-ne la identitat, 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.
> Les administracions públiques han de garantir que la utilització d'un dels sistemes que preveuen les lletres a) i b) sigui possible per a qualsevol procediment, encara que s'admeti per a aquest mateix procediment algun dels que preveu la lletra c).»

Així mateix, l'article 3.dos modifica l'apartat 2 de l'article 10 LPACAP, relatiu als sistemes de signatura dels interessats admesos en les seves relacions amb les administracions públiques, que queda redactat en els termes següents:

> «2. En cas que els interessats optin per relacionar-se amb les administracions públiques a través de mitjans electrònics, es consideren vàlids als efectes de signatura:

a) Sistemes de signatura electrònica qualificada i avançada basats en certificats electrònics qualificats de signatura electrònica expedits per prestadors inclosos a la ''Llista de confiança de prestadors de serveis de certificació''.
b) Sistemes de segell electrònic qualificat i de segell electrònic avançat basats en certificats electrònics qualificats de segell electrònic expedits per un prestador inclòs a la ''Llista de confiança de prestadors de serveis de certificació''.
c) Qualsevol altre sistema que les administracions públiques considerin vàlid en els termes i les condicions que s'estableixin, sempre que tinguin un registre previ com a usuari que permeti garantir-ne la identitat, 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.
Les administracions públiques han de garantir que la utilització d'un dels sistemes que preveuen les lletres a) i b) sigui possible per a tots els procediments en tots els seus tràmits, encara que addicionalment es permeti algun dels previstos a l'empara del que disposa la lletra c).»

La disposició transitòria primera del Reial decret llei preveu, en el seu apartat primer, el règim transitori de les modificacions introduïdes en l'article 3 RDL 14/2019 en relació amb els preceptes 9.2.*c* i 10.2.*c* LPACAP:

«1. Les entitats del sector públic que vulguin habilitar sistemes d'identificació o signatura de conformitat amb les lletres c) dels articles 9.2 i 10.2 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, a partir de l'entrada en vigor d'aquest Reial decret llei, han de sol·licitar l'autorització que preveuen els preceptes esmentats. Els sistemes que, abans de l'entrada en vigor esmentada, ja estiguin validats i

> plenament operatius en els procediments administratius de què es tracti no requereixen sotmetre's a aquesta autorització.»

Com s'ha exposat al principi d'aquest fonament jurídic, la sol·licitud de dictamen destaca que els títols aplicables a aquests preceptes són els articles 150 i 159 EAC, considerant que el Reial decret llei pot constituir una extralimitació i desbordar el títol estatal en matèria de seguretat pública, en la mesura que subjecta a autorització prèvia certs sistemes d'identificació i signatura electrònica.

L'escrit de sol·licitud demana també la disposició transitòria primera, per connexió, per la qual cosa el que es decideixi per a l'autorització prèvia prevista als articles 9.2.*c* i 10.2.*c* LPACAP serà igualment d'aplicació a la disposició transitòria primera.1 RDL 14/2019.

B) Als nostres efectes és rellevant procedir conjuntament a l'enquadrament competencial dels apartats u i dos de l'article 3 RDL 14/2019, ja que, com hem vist abans, és comú als dos, en tant que tenen una estructura idèntica, aplicada a la identificació electrònica o a la signatura, respectivament.

Primerament caldrà acudir a la disposició final primera RDL 14/2019, que és el precepte que menciona els títols competencials corresponents a cada article. Concretament, l'article 3 RDL 14/2019 es dicta segons la disposició precitada a l'empara de l'article 149.1.18 CE (bases del règim jurídic de les administracions públiques i procediment administratiu comú) i de l'article 149.1.29 CE (seguretat pública). De fet, se citen dos títols per al conjunt dels articles 3 i 4 RDL 14/2019. A continuació, farem una anàlisi d'altres elements que ens poden ajudar a destriar entre els dos títols competencials esmentats. Amb aquesta finalitat, ens referirem al preàmbul del RDL 14/2019 quan pertoqui.

Per una banda, el segon paràgraf de l'apartat VI del preàmbul situa la competència estatal en l'article 149.1.18 CE, en la mesura que modifica les principals lleis relatives al règim jurídic i al procediment administratiu comú de les administracions públiques, als nostres efectes la LPACAP. D'altra banda, el paràgraf quart cita expressament les modificacions dels articles 9.2.*c* i 10.2.*c* de la LPACAP, quant a «l'autorització prèvia necessària per part de l'Administració General de l'Estat dels sistemes d'identificació i signatura» i entén que estan habilitades per l'article 149.1.29 CE.

Segonament, la rúbrica general del RDL 14/2019 corrobora aquesta inicial dicotomia entre la finalitat de la disposició governativa, que té relació amb la seguretat pública (art. 149.1.29 CE), i el seu objecte, que, pel que ara ens interessa, és el relatiu a l'administració digital (art. 149.1.18 CE).

En aquest sentit, les referències generals del preàmbul del Reial decret llei també incideixen en els dos títols mencionats. Així, es diu que el desenvolupament i la utilització de les noves tecnologies a les administracions públiques precisen un marc jurídic que garanteixi la seguretat pública (apt. I, par. primer); s'exposa el caràcter estratègic de la seguretat pública pels riscos associats a les noves tecnologies, essent la ciberseguretat un dels àmbits prioritaris de la «seguretat nacional» (apt. I, par. segon i tercer), i, a l'últim, considera que l'administració electrònica estén la possibilitat d'atacs i d'activitats il·lícites que impacten en la seguretat pública (apt. I, par. cinquè).

En tercer lloc, més concretament sobre el contingut de l'article 3 RDL 14/2019, respecte del qual estem dictaminant, aquest precepte modifica, com hem dit, la LPACAP, dictada en virtut de l'article 149.1.18 CE d'acord amb la seva disposició final primera, que, pel que ara interessa, identifica expressament els títols competencials per establir les bases del règim jurídic de les administracions públiques i el procediment administratiu comú.

L'apartat primer d'aquest article 3 modifica l'article 9.2.*c* i l'apartat segon l'article 10.2.*c* LPACAP, els quals formen part del títol I, capítol II sobre identificació i signatura dels interessats en el procediment administratiu (a diferència de l'art. 40 LRJSP, que regula els sistemes d'identificació de les administracions públiques).

Novament, el preàmbul situa el contingut dels articles 3 i 4 RDL 14/2019 en relació amb les administracions públiques (apt. II, par. tercer), tot i que assenyala de forma explícita que la modificació de la lletra *c* de l'apartat segon dels articles 9 i 10 té com a finalitat garantir la seguretat pública (apt. II, par. sisè), qüestió que tractarem específicament més endavant.

a) L'article 3 RDL 14/2019 ha adaptat, amb un cert endarreriment, la regulació que modifica (LPACAP) al Reglament eIDAS (en vigor des de l'any 2014, i aplicable amb caràcter general des de l'1 de juliol de 2016), ja que, en cas que el legislador estimés necessària l'adaptació, ho podia haver fet àdhuc aprofitant l'aprovació de la mateixa LPACAP el 2015. Aquesta norma europea s'intitula i té per objecte el reconeixement dels sistemes d'identificació (art. 1.*a* Reglament eIDAS), essent necessària i mostrant reiteradament la seva preocupació per la seguretat tècnica dels sistemes (considerants 2, 12 i 19, entre d'altres). De fet, només en una ocasió es refereix a la protecció davant de possibles ciberatacs, en el considerant quart, quan s'esmenta la ciberdelinqüència com a obstacle a l'economia digital europea.

A banda d'aquesta norma europea, en els darrers anys la Unió Europea ha reforçat el seu marc normatiu en matèria de ciberseguretat. Així, per exemple, es va adoptar la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat a les xarxes i sistemes d'informació a la Unió, la qual, com veurem en el següent fonament jurídic,

ha estat transposada al nostre ordenament jurídic mitjançant el Reial decret llei 12/2018. I, en particular sobre la cooperació amb els estats membres i en l'àmbit de la defensa en aquesta àrea, recentment s'ha actualitzat el Marc polític de ciberdefensa de la Unió Europea, adoptat pel Consell el 19 de novembre de 2018, i s'ha aprovat el Reglament (UE) 2019/881 del Parlament Europeu i del Consell, de 17 d'abril de 2019, relatiu a ENISA (Agència de la Unió Europea per a la Ciberseguretat) i a la certificació de la ciberseguretat de les tecnologies de la informació i la comunicació i pel qual es deroga el Reglament (UE) 526/2013.

Des de la perspectiva del Reglament eIDAS, la identificació electrònica s'enfoca com un ventall de serveis públics electrònics que poden ser emprats per al reconeixement mutu entre els estats, sobre la base d'uns requisits mínims de seguretat de les xarxes (considerants segon, novè i catorzè). Els nivells de seguretat d'un sistema d'identificació electrònica depenen d'un conjunt de procediments tècnics (com ara la prova i verificació de la identitat o l'autentificació), d'activitats de gestió (entre les quals es pot assenyalar la de l'entitat que expedeix els mitjans d'identificació i el procediment per expedir-los) i dels controls aplicats (considerant setzè). El que no preveu, lògicament, el Reglament eIDAS són les autoritzacions, els informes o els controls entre administracions distintes dins d'un Estat membre, que és una de les novetats qüestionades per la sol·licitud de dictamen.

En tant que el Reial decret llei modifica la LPACAP en relació amb els sistemes d'identificació que admet, es podria considerar que es tracta de l'exercici de la competència reservada a l'Estat d'establir el procediment administratiu comú. Així mateix, els sistemes d'identificació dels administrats davant les administracions públiques constitueixen també un element del règim jurídic de les administracions públiques, on l'Administració valida els sistemes pels quals identifica els ciutadans i les empreses. Per això, la interrelació entre ciutadà i Administració és rellevant. En aquest cas, l'Estat

pot establir les bases amb una certa intensitat (art. 149.1.18 CE), més gran de la que pot establir quan l'objecte és *ad intra* de l'Administració (STC 50/1999, de 6 d'abril, FJ 3).

No obstant, pel que ara interessa, l'autorització prèvia per part del Ministeri de Política Territorial i Funció Pública constitueix un instrument de tutela que caldrà veure, d'acord amb la jurisprudència i la nostra doctrina, si és legítim en virtut d'algun títol competencial estatal. De fet, el RDL 14/2019 diu que l'autorització prèvia de l'Administració general de l'Estat, que eventualment pot ser denegada, d'acord amb un informe vinculant del Ministeri de l'Interior, es preveu per raó de seguretat pública, com indiquen el preàmbul (apt. VI, par. quart) i els articles 9.2.*c* i 10.2.*c* LPACAP.

Dins de les noves previsions sobre els sistemes d'identificació (art. 3.tres RDL 14/2019) s'inclou també la disposició addicional sisena LPACAP, amb dos apartats. El primer prohibeix autoritzar els sistemes d'identificació que emprin una tecnologia concreta, de registre distribuït, i els sistemes de signatura basada en l'anterior, disposició que sembla estar emparada en les bases de l'article 149.1.18 CE. La restricció és, en paraules del preàmbul, puntual i provisional, de manera que únicament es projecta en les relacions dels interessats amb l'Administració i fins l'aprovació d'un marc regulador (apt. II, par. novè preàmbul RDL 14/2019). El segon apartat imposa l'Estat com a autoritat intermèdia en l'ús de la citada tecnologia per garantir la seguretat pública (art. 149.1.29 CE). La sol·licitud no demana expressament la disposició addicional sisena, únicament en descriu succintament el contingut, i no n'argumenta la seva inconstitucionalitat o antiestatutarietat, per la qual cosa la introducció d'aquesta disposició del Reial decret llei a la LPACAP no serà objecte del nostre pronunciament.

A l'últim, la disposició transitòria primera del Reial decret llei es refereix a la implantació de l'article 3 RDL 14/2019 per les entitats del sector públic. Pel

que fa als sistemes d'identificació i signatura, la disposició transitòria primera.1 disposa que els que estiguin en funcionament, validats i plenament operatius, a l'entrada en vigor del Reial decret llei, no requereixen sotmetre's a l'autorització prèvia, mentre que els que es vulguin habilitar l'hauran de sol·licitar. Pel que fa al títol atribuïdor de competències, com que la disposició transitòria primera RDL 14/2019 només es refereix a la necessitat de demanar o no autorització prèvia a l'Administració general de l'Estat, el que es digui sobre aquesta qüestió valdrà per a aquesta disposició.

b) Finalment, abans d'enquadrar competencialment allò que interessa de l'article 3 RDL 14/2019, examinarem l'objectiu d'aquest precepte, per verificar si coincideix amb la matèria regulada i poder establir el títol competencial prevalent.

La finalitat de gran part de l'article 3 RDL 14/2019 és regular els sistemes d'identificació dels interessats admesos per les administracions públiques; per tant, la inserció és dins de l'article 149.1.18 CE. Tanmateix, en tres incisos, de les modificacions que aporta l'article 3 RDL 14/2019 (art. 9.2.*c*, 10.2.*c* i disp. add. sisena.2 LPACAP), es menciona incidentalment la seguretat pública com a element teleològic de part dels preceptes modificats.

El preàmbul, a banda d'assenyalar, com hem indicat abans, quin és l'objecte de la regulació (referida als art. 3 i 4 RDL 14/2019), la qual cosa ens porta al títol relatiu a les bases del règim jurídic de les administracions públiques i el procediment administratiu comú, també ens diu quina és la seva finalitat, que concreta incloent-hi també la de garantir la seguretat pública (apt. II, par. tercer).

A més, el RDL 14/2019 prescriu, en l'article 9.2.*c* LPACAP (sistemes d'identificació de clau concertada i altres), respecte a 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», sense que aquests últims s'indiquin en el text articulat. Dicció idèntica la trobem en l'article 10.2.*c* LPACAP (sistemes diferents dels de signatura i segell electrònics). Ambdós preceptes esmentats es modifiquen per garantir la seguretat pública, segons el preàmbul (apt. II, par. sisè), on s'intenta delimitar mínimament l'abast de la intervenció estatal. El proemi exposa que aquesta «té per objecte, exclusivament, verificar si el sistema validat tecnològicament per part de l'Administració o l'organisme públic de què es tracti pot produir o no afeccions o riscos a la seguretat pública, de manera que, si és així i només en aquest cas, l'Administració de l'Estat ha de denegar l'autorització sobre la base de les consideracions de seguretat pública esmentades», que no ha especificat.

No obstant això, la menció a la seguretat no apareix en la disposició transitòria primera sobre l'article 3 RDL 14/2019; ni en la intitulació del capítol II, que diu: «Mesures en matèria d'identificació electrònica davant les administracions públiques, ubicació de determinades bases de dades i dades cedides a altres administracions públiques»; ni en la rúbrica de l'article 3 RDL 14/2019, que és: «Modificació de la llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques», a diferència d'altres rúbriques d'altres capítols, on sí s'esmenta directament o indirecta (expressament als capítols IV i V; de forma tàcita en l'I, pel que fa a l'art. 1 RDL 14/2019, ja que és, com hem dit, la competència estatal que fonamenta la modificació i la norma modificada).

c) Entre aquests dos títols competencials (art. 149.1.18 i .29 CE) caldrà escatir doncs quin és el prevalent per al que a nosaltres ens interessa. Per això, caldrà definir-los breument.

Hem de descartar la reiterada competència en seguretat pública, perquè hi ha un ús excessivament expansiu en la utilització d'aquest títol competencial

sobre l'objecte del Reial decret llei. El Tribunal Constitucional, com hem avançat, ja ha delimitat restrictivament aquest concepte quan, en la STC 25/2004, de 26 de febrer, entre d'altres, ha afirmat que «no toda seguridad de personas y bienes, ni toda normativa encaminada a conseguirla o a preservar su mantenimiento, puede englobarse en aquélla, […] cuando es claro que se trata de un concepto más estricto en el que hay que situar de modo predominante las organizaciones y los medios instrumentales» (FJ 6), preservant necessàriament les competències autonòmiques (STC 184/2016, de 3 de novembre, FJ 3). A Catalunya, la garantia i protecció de la seguretat pública correspon dur-la a terme de forma ordinària a la policia de la Generalitat-Mossos d'Esquadra (DCGE 5/2017, de 29 de juny, FJ 3.4).

La seguretat pública és una expressió que cal acotar d'acord amb el context on se cita, atès que pot remetre a continguts tan diferents com la «seguretat nacional» (on intervé també la competència reservada a l'Estat per l'art. 149.1.4 CE) o la seguretat de les xarxes digitals (on pot incidir el títol competencial de l'art. 149.1.21 CE, relatiu a la competència estatal en telecomunicacions), ja que, en l'entorn de les administracions públiques, li escauria més aviat la denominada ciberseguretat circumscrita a l'administració electrònica (definida al DCGE 5/2017, FJ 2.1), la qual es tractaria tenint en compte la competència reservada a l'Estat per l'article 149.1.18 CE i que admet la potestat legislativa de les comunitats autònomes en el marc de les bases estatals.

La ciberseguretat, d'acord amb la STC 142/2018, de 20 de desembre, es concep com a un «conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan», definició a partir de la qual «fácilmente se infiere que, en tanto que dedicada a la seguridad de las tecnologías de la información, presenta un componente tuitivo», i es projecta sobre «el concreto ámbito de la protección de las redes

y sistemas de información que utilizan los ciudadanos, empresas y administraciones públicas» (FJ 4).

Donat el contingut dels diferents aspectes que configuren aquest concepte, s'entén que la ciberseguretat pot tenir diferents accepcions i estendre's a diverses activitats (STC 142/2018, FJ 4), per la qual cosa no és susceptible de ser reconduït a un sol títol competencial, entre els quals hi ha l'administració electrònica, per garantir la protecció de les xarxes de comunicacions electròniques que aquesta generi i dels drets dels administrats en les seves relacions amb l'Administració a través de mitjans electrònics (FJ 4 i 5). En aquest sentit, en el precitat DCGE 5/2017 distingíem tres accepcions: la que respon a situacions més greus, que s'identifica amb seguretat nacional; la que encaixa millor amb la seguretat pública, quan es tracti de la protecció de determinades infraestructures de telecomunicacions, i la referida a l'adopció de mesures ordinàries de seguretat respecte a la xarxa i, en general, a les tecnologies de la informació (FJ 2.1). Aquesta darrera accepció del terme també ha estat recollida a la jurisprudència constitucional (STC 142/2018, FJ 4, com a «medidas ordinarias de prevención o seguridad de la red y […] de las tecnologías de la información»), així com la ciberseguretat més greu, d'abast «nacional», la qual demanarà una intervenció estatal (art. 149.1.4 i .29 CE, i STC 184/2016, FJ 3 i 4).

La ciberseguretat, quan es refereix a il·lícits penals, resta fora de l'ordenació administrativa, però no tota protecció de la seguretat de les xarxes necessita una actuació policial i judicial penal. La competència *ex* article 149.1.29 CE estatal es troba limitada per les competències que les comunitats autònomes hagin assumit respecte de la creació de la seva pròpia policia (STC 148/2000, d'1 de juny, FJ 5).

Per la seva banda, les diferents administracions públiques són competents per a l'adopció de mesures d'autoprotecció en relació amb les seves infraestructures i la seguretat de les tecnologies de la informació i comunicació (STC 142/2018, FJ 5). De manera que la Generalitat «debe adoptar medidas en materia de ciberseguridad en tanto en cuanto se aplican a las relaciones que tiene con sus administrados y con otras administraciones, así como respecto de las infraestructuras tecnológicas, que pertenezcan a la estructura de la Administración de la Generalitat y a su sector público» (STC 142/2018, FJ 4). Així, la seguretat de les xarxes i dels sistemes de les tecnologies de la informació de l'Administració de la Generalitat seran protegides per aquesta, en virtut dels articles 159.1 i 150 EAC (DCGE 5/2017, FJ 2.2), essent la seva finalitat «prevenir les amenaces i les vulnerabilitats inherents a les seves xarxes interdependents i infraestructures de la informació, tant internament com en les seves relacions amb els administrats» (DCGE 5/2017, FJ 2.3).

Específicament, es vinculen a les polítiques de ciberseguretat les que poden desenvolupar el Govern i l'Administració de la Generalitat en relació amb la prestació dels serveis d'identificació electrònica i d'identitat i confiança digitals, a l'empara de les competències assumides pels articles 150 i 159 EAC (STC 142/2018, FJ 7), tal com vàrem dir en el DCGE 5/2017, FJ 3.5, on indicàvem que la competència principal de la Generalitat era la de l'article 159.1 EAC, afirmació que ratifiquem novament per als preceptes que estem dictaminant.

C) Un cop determinat que els apartats u i dos de l'article 3 RDL 14/2019 s'inscriuen dins la matèria del règim jurídic de les administracions i del procediment administratiu, definirem el règim competencial aplicable d'acord amb la Constitució i l'Estatut.

Segons el nostre parer, es tracta d'una regulació administrativa d'índole procedimental (la definició d'interessat es produeix dins d'un procediment administratiu), per a la qual cal una certa organització dels serveis electrònics que es posen a disposició dels interessats (els sistemes d'identificació i de signatura autoritzats), amb la consegüent adopció de mesures d'autoprotecció i de protecció dels drets dels ciutadans. Per tant, l'enquadrem prevalentment dins el 149.1.18 CE, tot i que hi pot incidir excepcionalment el títol de seguretat pública de l'article 149.1.29 CE (pel que fa a la ciberseguretat, en els termes que s'indicaran).

Per això, en el DCGE 5/2017, dèiem que:

> «En aquest marc en què la Generalitat concorre amb l'Estat per garantir la ciberseguretat en les comunicacions electròniques i els sistemes d'informació, hem d'afirmar que, […], caldrà distingir, com a criteri general, entre les [funcions] relatives a la prevenció dels incidents de ciberseguretat d'aquelles altres que comportin l'adopció de mesures reactives quan aquests s'hagin produït. I, encara més, dins d'aquest darrer tipus, ens caldrà diferenciar també, d'una banda, entre les mesures d'ordre tècnic que tinguin com a finalitat reparar, comprovar i restablir el normal funcionament de les comunicacions i els sistemes afectats i, de l'altra, les que s'adoptin com a reacció a una actuació que pugui suposar la comissió d'un acte que hagi de merèixer una sanció penal. Perquè, en ambdós supòsits, les conseqüències en l'ordre competencial […] seran diferents.» (FJ 3.1)

En aquest sentit, la competència sobre règim jurídic de les administracions públiques i procediment administratiu és una competència compartida en què incideix particularment l'article 159.1 EAC, en allò no afectat per l'article 149.1.18 CE: d'una banda, el 159.1.*a*, sobre mitjans necessaris per exercir funcions administratives, i, de l'altra, el 159.1.*c*, respecte del procediment administratiu derivat de les especialitats de l'organització de la Generalitat. No resulta directament aplicable, perquè no és el cas que ara dictaminem, la

creació d'òrgans administratius o les modalitats d'organització de l'Administració de la Generalitat (art. 150 EAC), tot i que aquesta competència també és reconeguda per la STC 142/2018, segons la qual permetria l'autoorganització per a «el diseño, creación y mantenimiento de "servicios de administración electrónica"» (FJ 6).

Sobre ciberseguretat i administració electrònica, ens hem de referir novament al DCGE 5/2017 (FJ 2.3), que sintetitza la jurisprudència constitucional i la nostra doctrina. En general, sobre l'article 149.1.18 CE hem de mencionar la STC 50/1999, de 6 d'abril (FJ 3), en relació amb les competències de l'Estat per fixar les bases del règim jurídic de les administracions públiques, on són referència igualment el DCGE 24/2015, de 17 de desembre, FJ 4, i la STC 132/2018, de 13 de desembre, FJ 4. I, pel que fa al procediment administratiu comú, cal fer esment al DCGE 23/2015, de 17 de desembre, FJ 2 i 3, i a la STC 55/2018, de 24 de maig, FJ 4 i 9.

Pel que fa al règim jurídic de les administracions públiques, aquest títol competencial permet «establecer los elementos esenciales que garanticen un régimen jurídico unitario aplicable a todas las Administraciones públicas» (STC 50/1999, 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, FJ 4).

Sobre això, cal recordar que la intensitat de les bases fixades per l'Estat és diversa. Així, la legislació bàsica estatal *ex* article 149.1.18 CE, com a límit a les competències de la Generalitat *ex* article 159.1 EAC, no té la mateixa extensió ni intensitat quan es tracta d'aspectes merament organitzatius interns, que no afecten directament l'activitat externa de l'Administració ni els administrats, que quan, per contra, es tracta d'altres aspectes en què sí

que es dona aquesta afectació (STC 50/1999, FJ 3, i DCGE 5/2017, FJ 3.5). El Tribunal Constitucional determina que la densitat de les bases «podrá ser tanto mayor cuanto más directa sea la finalidad de garantizar un trato común a los ciudadanos en sus relaciones con la Administración» (STC 50/1999, FJ 3, i 132/2018, FJ 4).

En qualsevol cas, les bases de l'article 149.1.18 CE, sigui quina sigui la seva finalitat, no poden tenir un nivell de detall o completesa que pràcticament impedeixi l'adopció de polítiques pròpies autonòmiques (STC 130/2013, de 4 de juny, FJ 6), facultat que també reconeix l'article 111 EAC a la Generalitat en les matèries de competència compartida.

A més, cal tenir present que el Reglament eIDAS fixa uns continguts essencials per a les especificacions tècniques mínimes, normes i procediments a fi de determinar els nivells de seguretat de la identificació electrònica, en referència a la seva fiabilitat i qualitat (art. 8.3 Reglament eIDAS). Igualment, 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 sobre les bases del règim jurídic de les administracions públiques, defineix les mesures de seguretat mínimes que les administracions hauran d'aplicar en relació amb la identificació, l'autenticació i la firma electrònica, les quals poden ser ampliades segons les circumstàncies del cas concret.

En el DCGE 23/2015 hem recordat que la competència de l'Estat sobre el procediment administratiu comú «és l'aspecte del títol competencial *ex* article 149.1.18 CE més directament concernit per l'objecte de la Llei 39/2015» (FJ 2). El Tribunal Constitucional, en la STC 166/2014, de 22 d'octubre, ressalta l'adjectiu «comú», entenent que «lo que el precepto constitucional ha querido reservar en exclusiva al Estado es la determinación de los principios o normas que, por un lado, definen la estructura general del

iter procedimental que ha de seguirse para la realización de la actividad jurídica de la Administración y, por otro, prescriben la forma de elaboración, los requisitos de validez y eficacia, los modos de revisión y los medios de ejecución de los actos administrativos, incluyendo señaladamente las garantías generales de los particulares en el seno del procedimiento» (FJ 4), però, alhora, indica que no s'inclou en aquesta matèria competencial «toda regulación que de forma indirecta pueda tener alguna repercusión o incidencia en el procedimiento así entendido» (STC 50/1999, FJ 3).

L'Estat, d'acord amb la STC 166/2014, no pot interferir en l'organització interna de les comunitats autònomes:

> «señalando los órganos competentes para determinados trámites […] o imponiendo órganos estatales de control frente a los propios de las Comunidades Autónomas […] o, en general, establecer una regla competencial "específica en la materia" […], pues lo que sí tienen éstas reservado es la regulación de las "normas ordinarias de tramitación del procedimiento"» (FJ 5).

En l'esmentat Dictamen vam referir-nos als articles 9.2 i 10.2 LPACAP, en la seva redacció original, sense la incorporació de la tutela estatal que ara examinem, no trobant-hi tatxa d'inconstitucionalitat o antiestatutarietat, perquè les dues llistes de confiança de prestadors de serveis de certificació a les quals es refereixen aquests preceptes i que llavors es discutia «no són un *numerus clausus*, ans al contrari, ja que, com s'expressa en el supòsit de la lletra *c* dels paràgrafs corresponents dels dos articles examinats, s'admet en darrer terme qualsevol altre sistema que les administracions públiques considerin vàlid, en els termes i les condicions que s'estableixin, i, consegüentment, cada Administració pot adoptar un d'aquests "altres sistemes" i regular convenientment els termes i les condicions corresponents per al seu ús i la seva validesa» (FJ 3.1).

La STC 55/2018 va descriure l'article 9 LPACAP a l'efecte de resoldre la impugnació del seu apartat tercer, per la qual cosa no va entrar en la redacció anterior de l'apartat segon, que ara dictaminem modificat (ni tampoc en l'article 10, que no va ser impugnat), i que tenia una redacció més respectuosa amb l'autonomia, apreciada pel Tribunal, des de la perspectiva del marge que es permetia per definir els sistemes d'identificació electrònica en el si del procediment administratiu. Així, el Tribunal diu que la regulació (abans de ser modificada) afavoria que cada administració dissenyés els seus propis sistemes d'identificació electrònica i n'admetés d'altres expedits per altres entitats. De manera que hi tenien cabuda polítiques diverses, dotades de més a menys nivell de seguretat, i, a més, garantia un tractament comú a tots els ciutadans perquè s'havien de poder emprar els sistemes admesos per l'Estat. En aquests termes, el Tribunal conclou que la regulació llavors examinada no desbordava els límits de l'article 149.1.18 CE ni envaïa les competències autonòmiques en matèria d'organització i procediment administratiu (FJ 9).

Aquest és, doncs, el paràmetre competencial que hem d'aplicar en relació amb la preservació de la seguretat en l'Administració electrònica de la Generalitat quant a la identificació i signatura electrònica dels interessats davant aquesta Administració pública.

D) La qüestió debatuda respecte els articles 9.2.*c* i 10.2.*c* LPACAP se centra en l'autorització prèvia que el Reial decret llei atribueix a l'Administració general de l'Estat en termes idèntics per a tots dos preceptes. La Secretaria General d'Administració Digital del Ministeri de Política Territorial i Funció Pública és l'òrgan estatal habilitat per efectuar dita autorització. La Secretaria d'Estat de Seguretat del Ministeri de l'Interior haurà d'incorporar a l'autorització un informe vinculant que pot determinar-ne la denegació només per motius de seguretat pública. Això no obstant, l'autorització s'ha

d'emetre en el termini màxim de tres mesos. En cas contrari, i sense perjudici de l'obligació de resoldre dins del termini, la manca de resolució tindrà efectes desestimatoris.

D'acord amb el paràmetre competencial que hem establert, l'Estat només pot establir bases, és a dir, un conjunt de principis i regles per assegurar un tractament comú dels interessats. En el supòsit que dictaminem, la potestat legislativa de la Generalitat per establir els sistemes validats s'ha condicionat pels subapartats *a* i *b* dels articles 9.2 i 10.2 LPACAP. Efectivament, aquests subapartats s'han de posar en relació amb el segon paràgraf dels articles 9.2.*c* i 10.2.*c*, de manera que les administracions han de garantir que es puguin utilitzar els sistemes previstos en les dites lletres en qualsevol tràmit del procediment. Oimés, l'article 9.4 LPACAP determina que els sistemes que siguin acceptats per l'Administració estatal serviran per acreditar les identificacions dels interessats davant de les altres administracions, sense reciprocitat. Igualment, els articles 9.2.*c* i 10.2.*c* LPACAP estableixen l'obligació que els usuaris estiguin registrats prèviament per garantir-ne la identitat, requisit que abans de la reforma introduïda pel Reial decret llei s'ubicava a la part general dels articles 9.2 i 10.2 i era aplicable, per tant, a tots els sistemes d'identificació i signatura previstos.

L'autorització estatal prèvia introduïda per l'article 3.u i .dos RDL 14/2019 no s'adiu amb el que permet l'article 149.1.18 CE, en la mesura que no constitueix una base del règim jurídic de les administracions públiques per la seva estructura normativa, ni un element que ha de ser necessàriament comú del procediment administratiu, atès que el mínim comú normatiu ja es garanteix mitjançant els sistemes d'identificació admesos per l'Estat, com ha estat dit.

Així, com hem exposat abans, aquest títol competencial permet establir els elements essencials que asseguren un règim jurídic unitari aplicable a totes

les administracions, amb major amplitud en tant que tracti aspectes que afecten directament l'activitat externa de l'Administració i dels administrats, amb la finalitat de garantir un tractament comú als ciutadans en les seves relacions amb l'Administració (STC 50/1999, FJ 3, i 132/2018, FJ 4).

Tanmateix, la previsió qüestionada per la sol·licitud de dictamen constitueix més aviat una tutela o un control sobre l'administració autonòmica, en relació amb els quals hi ha una extensa doctrina constitucional, que tindrem en compte en relació amb el cas que dictaminem, després de recordar breument els criteris principals emprats per la jurisprudència i en la nostra tasca dictaminadora que més ens interessen respecte d'aquesta qüestió.

Primerament, cal dir que no existeix en l'Estat de les autonomies dissenyat per la Constitució una institució general de control de l'Estat sobre les comunitats autònomes, sinó una pluralitat de procediments específics, de caràcter i efectes diversos. Aquests mecanismes i instruments de control d'una instància central sobre una altra d'autonòmica es recullen a la Constitució, bàsicament a l'article 153 CE, però també els podem trobar en altres preceptes constitucionals (art. 150 i 161.2 CE, entre d'altres) o en el bloc de la constitucionalitat (STC 6/1982, de 22 de febrer, FJ 7; 76/1983, de 5 d'agost, FJ 12, i STC 79/2017, de 22 de juny, FJ 17).

Així mateix, la STC 118/1996, de 27 de juny, FJ 18, afirma que l'autonomia prevista constitucionalment (art. 2, 137 i 156 CE) no és compatible amb un control d'oportunitat política que pugui implicar una substitució de la voluntat de les institucions autonòmiques per la de l'Estat (en el DCGE 19/2015, de 26 de novembre, FJ 2.7, resumim la jurisprudència sobre la qüestió) si no és previst a la Constitució, als estatuts o a les lleis orgàniques del bloc de la constitucionalitat (STC 6/1982, FJ 7), que delimiten constitucionalment les competències. D'altra manera es constituiria una situació de dependència jeràrquica de les comunitats autònomes respecte de l'Administració estatal

contrària al principi d'autonomia (STC 76/1983, FJ 12) i es legitimaria un tipus de control sobre l'Administració autonòmica que no s'adequaria al repartiment competencial entre l'Estat i les comunitats autònomes (DCGE 21/2014, de 30 de setembre, FJ 3.4).

L'Estat «ja disposa de mitjans per assegurar el compliment per part de les comunitats autònomes de les seves obligacions, tot respectant la posició institucional d'aquestes, havent-se d'abstenir d'utilitzar mètodes de control jeràrquic i de limitar-se als instruments expressament previstos per la Constitució, singularment els de caràcter general de l'article 153 CE» (DCGE 21/2014, FJ 3.4), com ara una comunicació prèvia o sistemes de col·laboració.

D'altra banda, el Tribunal Constitucional distingeix entre els controls jurisdiccionals i els administratius. Aquests darrers poden ser a la vegada *ex ante* o *ex post* a l'adopció de la decisió. Dins dels controls administratius previs, el Tribunal Constitucional ha admès la tècnica dels informes vinculants com a mitjà d'integració de dues competències concurrents de titularitat autonòmica i estatal (STC 79/2017, de 22 de juny, FJ 17). Així, a partir de la STC 18/2011, de 3 de març, el Tribunal afirma que:

> «la intervención del Estado mediante la técnica del informe preceptivo y vinculante debe reputarse constitucionalmente legítima cuando se funde en el ejercicio de una competencia propia sobre una determinada materia (…) que le habilite para actuar, distinta de la materia sobre la cual la Comunidad Autónoma ejerce su propia competencia de autorización.» (FJ 21.*a*)

A més a més, el Tribunal Constitucional ha indicat que els controls que s'exerceixin constitucionalment sobre les autonomies no poden ser genèrics ni indeterminats (des de la STC 4/1981, de 2 de febrer, FJ 3, i, més recentment, STC 85/2016, de 28 d'abril, FJ 5), sinó que han de ser concrets i

precisos (STC 154/2015, de 9 de juliol, FJ 6.*b*). Així, en cas d'admetre algun instrument de vigilància de les comunitats autònomes ha de ser sobre la base de competències estatals de coordinació, previstes constitucionalment. En aquests casos, la intervenció administrativa ha d'estar suficientment objectivada o determinada en normes de rang legal (STC 14/2018, de 20 de febrer, FJ 10.*d*).

L'autorització estatal prevista als articles 9.2.*c* i 10.2.*c* LPACAP s'adiu amb la tutela de caràcter previ, segons els esmentats preceptes, de manera que és una actuació exigida abans de qualsevol decisió de validació o no dels sistemes de clau concertada o d'altres que realitzi l'Administració de la Generalitat. Aquest fet, per si mateix, amb independència del sentit de l'autorització estatal, condiciona el procediment administratiu autonòmic de resolució.

Com acabem de dir, els informes previs preceptius i vinculants només són legítims si se suporten en una competència estatal. Només són admissibles quan efectivament es doni aquesta projecció de la competència estatal i es resolguin basant-se en aquesta competència (STC 18/2011, FJ 21.*a*, i DCGE 7/2014, de 27 de febrer, FJ 3.3).

Hem descartat que sigui d'aplicació aquí el títol competencial de seguretat pública, que, com hem dit en relació amb la ciberseguretat, no és una matèria reservada exclusivament a l'Estat, ja que en l'administració digital intervé fonamentalment la seguretat ordinària de les xarxes, la qual encaixa més en el règim competencial resultant del binomi articles 149.1.18 CE i 159 EAC, dins de la matèria de règim jurídic de les administracions públiques i del procediment administratiu. Camp en què les previsions d'autorització prèvia de l'article 9.2.*c* LPACAP, reiterada en el 10.2.*c*, no hi tenen cabuda, perquè no és un control emparat per les bases estatals ni per l'establiment d'un procediment comú, com ha estat indicat. Aquesta previsió del Reial

decret llei interfereix en la competència de la Generalitat de permetre autoritzar sistemes, fins a poder-l'hi impedir. Certament, l'article 3 RDL 14/2019 fa dependre la decisió de la Generalitat de la de l'Administració general de l'Estat, sense que aquesta disposi de competències sobre l'autorització dels sistemes d'identificació dels interessats davant l'Administració catalana.

En un cas proper, en matèria de serveis d'administració electrònica (en l'àmbit de l'art. 149.1.18 CE), el Tribunal Constitucional, en la STC 55/2018, considera inconstitucional que l'Administració estatal condicioni, amb una certa dosi d'indefinició, la creació o el manteniment de plataformes electròniques autonòmiques a la presentació davant del Ministeri estatal de la seva justificació en termes d'eficiència si la decisió autonòmica queda supeditada a la valoració estatal de la justificació aportada (FJ 11). Més recentment, abona la inconstitucionalitat d'una intermediació estatal, perquè pot produir pertorbacions en el funcionament de l'Administració autonòmica, situant-la de forma subordinada i dependent d'una actuació aliena (STC 33/2018, de 12 d'abril, FJ 11).

En aquest sentit, l'autorització prèvia estatal, de la Secretaria General d'Administració Digital del Ministeri de Política Territorial i Funció Pública, no ve predeterminada a la norma per uns motius concrets i precisos i, ultra això, té unes conseqüències inadequades, ja que, en el cas de pronunciar-se negativament la Secretaria d'Estat de Seguretat del Ministeri de l'Interior, els efectes són denegatoris i en el supòsit que no doni resposta dins de termini, s'entén que la resolució és desestimatòria.

Igualment, la disposició transitòria primera.1 RDL 14/2019, en exigir aquesta autorització prèvia a partir de l'entrada en vigor d'aquest RDL 14/2019 a les entitats del sector públic que vulguin habilitar sistemes d'identificació o

signatura, ha de seguir la mateixa sort que l'article 3.u i .dos, en relació amb els articles 9.2.*c* i 10.2.*c* LPACAP.

En conseqüència, l'autorització prèvia prevista a l'article 3.u i .dos RDL 14/2019, amb informe vinculant i efecte de silenci desestimatori, constitueix un control il·legítim i vulnera les competències de la Generalitat sobre l'organització i la seguretat de les seves xarxes (art. 159 EAC) i no està emparada pel títol competencial sobre les bases del règim jurídic de les administracions públiques i del procediment administratiu comú, ni tampoc pel de seguretat pública (art. 149.1.18 i .29 CE).

En conclusió, l'article 3.u i .dos RDL 14/2019, en la modificació dels articles 9.2.*c* i 10.2.*c* LPACAP, 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 està emparat per l'article 149.1.18 i .29 CE. Per connexió, també les vulnera la disposició transitòria primera.1 RDL 14/2019, la qual tampoc troba empara en els preceptes constitucionals citats.

Així mateix, també per connexió, per interpretació sistemàtica d'aquest precepte, hem d'arribar a la mateixa conclusió d'inconstitucionalitat i antiestatutarietat respecte de la disposició final primera, apartat 2, RDL 14/2019, en la mesura que fonamenta la competència de l'Estat per dictar l'article 3.u i .dos del RDL 14/2019 en els títols competencials de l'article 149.1.18 i .29 CE.

Quart. L'examen de constitucionalitat i d'estatutarietat dels preceptes del Reial decret llei 14/2019 relatius a les telecomunicacions

En aquest fonament jurídic analitzarem els preceptes del Reial decret llei objecte de dictamen que contenen mesures dirigides a reforçar la seguretat en matèria de telecomunicacions. En concret, en vista dels dubtes enunciats a la sol·licitud, i per la seva connexió temàtica, tractarem en primer lloc els apartats u i cinc de l'article 6 RDL 14/2019, que reformen els articles 4.6 i 81.1 de la Llei 9/2014, de 9 de maig, general de telecomunicacions (en endavant, LGTEL), respectivament. Seguidament, l'apartat dos del mateix article 6 i la disposició addicional única RDL 14/2019, que introdueixen un nou apartat 3 a l'article 6 LGTEL i el seu règim transitori. Finalment, durem a terme l'examen de l'article 7 RDL 14/2019, sobre mesures per reforçar la coordinació en matèria de seguretat de les xarxes i els sistemes d'informació, que incorpora un apartat 3 a l'article 11 del Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació.

1. L'apartat u de l'article 6 RDL 14/2019 modifica l'apartat 6 de l'article 4 de la Llei 9/2014, de 9 de maig, general de telecomunicacions, que queda redactat de la manera següent:

> «6. El Govern, amb caràcter excepcional i transitori, pot acordar l'assumpció per l'Administració General de l'Estat de la gestió directa o la intervenció de les xarxes i els serveis de comunicacions electròniques en determinats supòsits excepcionals que puguin afectar l'ordre públic, la seguretat pública i la seguretat nacional. En concret, aquesta facultat excepcional i transitòria de gestió directa o intervenció pot afectar qualsevol infraestructura, recurs associat o element o nivell de la xarxa o del servei que sigui necessari per

> preservar o restablir l'ordre públic, la seguretat pública i la seguretat nacional.
>
> Així mateix, en cas d'incompliment de les obligacions de servei públic a què es refereix el títol III d'aquesta Llei, el Govern, amb l'informe previ preceptiu de la Comissió Nacional dels Mercats i la Competència, i igualment amb caràcter excepcional i transitori, pot acordar l'assumpció per l'Administració General de l'Estat de la gestió directa o la intervenció dels serveis corresponents o de l'explotació de les xarxes corresponents.
>
> Els acords d'assumpció de la gestió directa del servei i d'intervenció d'aquest o els d'intervenir o explotar les xarxes a què es refereixen els paràgrafs anteriors els ha d'adoptar el Govern per iniciativa pròpia o a instància d'una Administració pública competent. En aquest últim cas, cal que l'Administració pública tingui competències en matèria de seguretat o per a la prestació dels serveis públics afectats pel funcionament anormal del servei o de la xarxa de comunicacions electròniques. En el supòsit que el procediment s'iniciï a instància d'una Administració diferent de la de l'Estat, aquesta té la consideració d'interessada i pot evacuar un informe amb caràcter previ a la resolució final.»

A) Per tal de poder identificar la finalitat i el contingut d'aquest precepte, cal prèviament situar-lo en el seu context normatiu, com també delimitar quin és el seu àmbit d'aplicació, així com fer esment d'alguns altres conceptes i qüestions generals de la matèria de les telecomunicacions que hi tenen una relació directa, tal com es desprèn de la seva mateixa configuració legal. Seguidament, a fi de poder precisar els efectes perseguits pel legislador estatal, resultarà convenient fixar-nos en la versió anteriorment vigent de l'article 4, apartat 6, LGTEL i assenyalar els principals canvis que ha experimentat el seu redactat amb la reforma que és objecte d'aquest Dictamen.

D'entrada, doncs, cal recordar que l'article 4.6 s'insereix en la LGTEL, l'àmbit d'aplicació de la qual és «la regulació de les telecomunicacions, que

comprenen l'explotació de les xarxes i la prestació dels serveis de comunicacions electròniques i els recursos associats» (art. 1.1 LGTEL). Val a dir que la Llei delimita el seu àmbit d'aplicació per exclusió, és a dir, a partir de l'enumeració d'un seguit de serveis que resten fora del seu abast: els serveis de comunicació audiovisual, els continguts audiovisuals transmesos mitjançant les xarxes, el règim bàsic dels mitjans de comunicació social de naturalesa audiovisual, els serveis que subministrin continguts transmesos mitjançant xarxes i serveis de comunicacions electròniques, les activitats que consisteixen en l'exercici del control editorial sobre els dits continguts i els serveis de la societat de la informació, actualment regulats a la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (en endavant, LSSI), sempre que no consisteixin, en la seva totalitat o principalment, en el transport de senyals a través de xarxes de comunicacions electròniques (art. 1.2 LGTEL). En aquest sentit, cal indicar que un servei de la societat de la informació és el que es presta normalment a títol onerós, a distància, per via electrònica i a petició individual del destinatari, com, per exemple, la contractació de béns o serveis, l'organització i gestió de subhastes, la gestió de compres, la tramesa de comunicacions comercials o el subministrament d'informació per via telemàtica (annex *a* LSSI).

Per tant, per dotar de significat l'expressió «xarxes i serveis de comunicacions electròniques» sobre els quals recauen les mesures previstes al nou article 4.6 LGTEL, hem d'acudir en primer terme a les definicions que conté l'annex II de l'esmentada Llei i, complementàriament, entre d'altres, a la Directiva (UE) 2018/1972 del Parlament Europeu i del Consell, d'11 de desembre de 2018, per la qual s'estableix el Codi europeu de les comunicacions electròniques. A tall de síntesi, d'una banda, són «xarxes de comunicacions electròniques» els sistemes de transmissió i, quan escaigui, altres recursos que permetin el transport de senyals mitjançant cables, ones hertzianes, mitjans òptics o altres mitjans electromagnètics, amb inclusió de

les xarxes de satèl·lits, xarxes terrestres fixes (de commutació de circuits i de paquets, inclosa internet) i mòbils, sistemes de línia elèctrica, en la mesura que s'utilitzin per a la transmissió de senyals, xarxes utilitzades per a la radiodifusió sonora i televisiva i xarxes de televisió per cable, independentment del tipus d'informació transportada (annex II.31 LGTEL). De la mateixa manera, és una «xarxa pública de comunicacions electròniques» la que s'empra, en la seva totalitat o principalment, per a la prestació de serveis de comunicacions electròniques disponibles per al públic i que suporta la transferència d'informació entre punts de terminació de la xarxa (art. 2.8 Directiva [UE] 2018/1972).

I, de l'altra, són «serveis de comunicacions electròniques» els prestats «en general a canvi d'una remuneració que consisteix, en la seva totalitat o principalment, en el transport de senyals a través de xarxes de comunicacions electròniques, amb inclusió dels serveis de telecomunicacions i serveis de transmissió en les xarxes utilitzades per a la radiodifusió» (annex II.35). Segons la Directiva (UE) 2018/1972, els serveis de comunicacions electròniques comprenen els següents tipus de serveis (art. 2.4): a) el «servei d'accés a internet», entès com aquell servei de comunicacions electròniques a disposició del públic que proporciona accés a internet i, per tant, connectivitat entre pràcticament tots els punts extrems connectats a internet, amb independència de la tecnologia de xarxa i de l'equip terminal utilitzats (art. 2.2 del Reglament [UE] 2015/2120 del Parlament Europeu i del Consell, de 25 de novembre de 2015, pel qual s'estableixen les mesures en relació amb l'accés a una internet oberta); b) el «servei de comunicacions interpersonals», que és el que permet l'intercanvi interpersonal i interactiu d'informació (entre un nombre finit de persones físiques) i que comprèn serveis com les trucades de veu tradicionals entre dues persones, així com també tot tipus de correus electrònics, serveis de missatgeria o xerrades en grup, restant-ne exclosos, doncs, la radiodifusió lineal, el vídeo a la carta, els llocs web, les xarxes socials, els blogs o l'intercanvi d'informació entre

màquines (considerant 17), i c) els serveis consistents, en la seva totalitat o principalment, en el transport de senyals, com és el cas dels serveis de transmissió utilitzats per a la prestació de serveis màquina a màquina (tals com els vehicles connectats) i per a la radiodifusió.

Aquests conceptes, a la Llei, es completen, d'una banda, amb els dels recursos associats a les xarxes i als serveis de comunicacions electròniques que, de manera resumida, comprenen les infraestructures físiques, els sistemes, els dispositius i altres recursos o elements associats a una xarxa o a un servei que permetin o donin suport a la prestació de serveis a través de la dita xarxa o el dit servei o tinguin potencial per a això (inclouen, entre d'altres, edificis, entrades a aquests o el seu cablejat i altres construccions de suport, conductes, distribuïdors, etc.). I, de l'altra, amb serveis associats a unes i altres, com ara la traducció de números, els sistemes d'accés condicional i les guies electròniques de programes o serveis d'identitat, localització i presència (annex II, LGTEL, núm. 30 i 34, respectivament).

Certament, la regulació de les telecomunicacions no comprèn els continguts dels serveis prestats a través de les xarxes i els serveis de comunicació electrònica, com són els continguts de radiodifusió televisiva i sonora, els serveis financers i els serveis de la societat de la informació, ja que, en relació amb els darrers, les mesures adoptades tenen com a finalitat principal preservar la llibertat d'expressió i d'informació, la diversitat cultural i lingüística, el pluralisme dels mitjans de comunicació, la imparcialitat, la inclusió social, la protecció dels menors o la dels consumidors. Però és evident que la separació de la regulació de les comunicacions electròniques i la regulació dels continguts, sovint de difícil delimitació, no permet ignorar la convergència d'ambdós sectors ni els vincles que existeixen entre ells (considerants 7 i 10 Directiva [UE] 2018/1972), com tampoc es pot obviar que les xarxes i els serveis de comunicacions electròniques actuen com a via d'entrada als continguts i a la societat de la informació. Així, per exemple, un

mateix operador de cable pot oferir un servei de comunicacions electròniques, com el transport de senyals televisius i serveis de la societat de la informació no sotmesos a la LGTEL, de manera que es poden imposar a aquesta empresa obligacions addicionals en relació amb la seva activitat com a proveïdor o distribuïdor de continguts (considerant 11 Directiva [UE] 2018/1972).

Aquesta convergència i la consideració de les xarxes i els serveis de comunicacions electròniques com a canals imprescindibles de la comunicació i la informació, que, a més, manegen dades de caràcter personal en la gestió dels serveis que presten, es confirma en el fet mateix que el legislador estatal ha establert un conjunt de procediments i cauteles per a la protecció dels drets fonamentals i la preservació d'altres béns i drets constitucionals (p. ex., la seguretat pública) que poden resultar afectats en els supòsits en què s'hagin de realitzar mesures limitatives sobre les xarxes i els serveis dits, els quals s'incorporen a l'estatut mateix dels operadors de telecomunicacions. En concret, ens referim a la prolixa regulació continguda al capítol III, del títol III, de la LGTEL (art. 39 i seg.), sobre el secret de les comunicacions i la protecció de dades personals i drets i obligacions de caràcter públic vinculats amb les xarxes i els serveis de comunicacions electròniques.

Per finalitzar amb aquesta caracterització de les xarxes i els serveis de comunicacions electròniques, cal recordar que les telecomunicacions es qualifiquen com a serveis d'interès general que es presten en lliure competència (art. 2.1 LGTEL), pel fet que satisfan necessitats bàsiques o fonamentals i constitueixen un factor clau per al desenvolupament econòmic, social i personal, de forma que han de respondre alhora als principis de continuïtat, universalitat, igualtat d'accés i transparència (en aquest sentit, Protocol 26 del TFUE sobre serveis d'interès general, art. 1).

A fi de garantir l'existència de serveis de comunicacions electrònics disponibles per al públic, d'adequada qualitat en tot el territori a través d'una competència i una llibertat d'elecció reals, com també per fer front a les circumstàncies en què el mercat no pugui atendre satisfactòriament les necessitats dels usuaris finals, són exigibles als operadors un conjunt d'obligacions de servei públic en l'explotació de xarxes públiques i en la prestació de serveis de comunicacions electròniques (art. 23 LGTEL). Respecte a les categories d'aquestes obligacions de servei públic (art. 24 LGTEL), la Llei distingeix entre l'«obligació de servei universal», que garanteix la prestació del servei a tots els usuaris finals amb independència de la seva localització geogràfica, amb una qualitat determinada i a un preu assequible (art. 25 a 27 LGTEL), i altres obligacions de servei públic, que el Govern pot imposar addicionalment als operadors per raons d'interès general, com ara per necessitats de la defensa nacional, la seguretat pública, la seguretat viària o quan es tracti de serveis que afectin la seguretat de les persones o la protecció civil (art. 28 LGTEL).

Altrament, només tenen ja la consideració més tradicional de «servei públic» els serveis per a la defensa nacional, la seguretat pública, la seguretat viària i la protecció civil (art. 4 LGTEL).

B) Fetes les consideracions anteriors, cal assenyalar que l'actual apartat 6 de l'article 4 LGTEL té el seu antecedent a la Llei general de telecomunicacions 11/1998, de 24 d'abril (llavors art. 5.5), amb un contingut que s'ha mantingut pràcticament invariable al llarg dels anys en les diferents lleis de telecomunicacions aprovades (art. 4.5 Llei 32/2003, de 3 de novembre, general de telecomunicacions i, actualment, art. 4.6 LGTEL) fins a la nova redacció donada pel Reial decret llei 14/2019, que ara es dictamina.

A efectes indicatius, reproduïm a continuació la redacció fins ara vigent de l'article 4.6 LGTEL (derogada pel RDL 14/2019), que deia:

> «6. El Govern, amb caràcter excepcional i transitori, pot acordar l'assumpció per l'Administració General de l'Estat de la gestió directa de determinats serveis o de l'explotació de determinades xarxes de comunicacions electròniques, d'acord amb el text refós de la Llei de contractes del sector públic, aprovat pel Reial decret legislatiu 3/2011, de 14 de novembre, per garantir la seguretat pública i la defensa nacional. Així mateix, en cas d'incompliment de les obligacions de servei públic a què es refereix el títol III d'aquesta Llei, el Govern, amb l'informe previ preceptiu de la Comissió Nacional dels Mercats i la Competència, i igualment amb caràcter excepcional i transitori, pot acordar l'assumpció per l'Administració General de l'Estat de la gestió directa dels serveis corresponents o de l'explotació de les xarxes corresponents. En aquest últim cas, pot, amb les mateixes condicions, intervenir la prestació dels serveis de comunicacions electròniques.
>
> Els acords d'assumpció de la gestió directa del servei i d'intervenció d'aquest o els d'intervenir o explotar les xarxes a què es refereix el paràgraf anterior s'han d'adoptar pel Govern per iniciativa pròpia o a instància d'una administració pública competent. En aquest últim cas, cal que l'Administració pública tingui competències en matèria de seguretat o per a la prestació dels serveis públics afectats pel funcionament anormal del servei o de la xarxa de comunicacions electròniques. En el supòsit que el procediment s'iniciï a instància d'una administració diferent de la de l'Estat, aquesta té la consideració d'interessada i pot evacuar un informe amb caràcter previ a la resolució final.»

De la lectura del precepte transcrit es desprèn que, abans, el Govern podia acordar, amb caràcter excepcional i transitori, que l'Administració general de l'Estat assumís la gestió directa de *determinats* serveis o de l'explotació de *certes* xarxes de comunicacions electròniques d'acord amb el que preveia la legislació en matèria de contractació pública; en concret, la llavors vigent Llei de contractes del sector públic, aprovada pel Reial decret legislatiu 3/2011, de 14 de novembre.

El legislador establia aquesta possibilitat per a dues situacions diferents. D'una banda, el Govern podia adoptar l'esmentat acord quan fos necessari per garantir la seguretat pública i la defensa nacional (primer incís del precepte). I, de l'altra, ja fos per pròpia iniciativa o a instància de l'administració autonòmica competent en matèria de seguretat o per a la prestació dels serveis públics afectats, i amb l'informe previ de la Comissió Nacional dels Mercats i de la Competència, quan l'operador de telecomunicacions incomplís les obligacions de servei públic imposades pel legislador en la gestió del servei o l'explotació de les xarxes de comunicacions electròniques (incís segon), atesa la seva condició de serveis econòmics d'interès general (art. 23 a 28 del títol III, LGTEL). En aquest darrer supòsit d'incompliment de les obligacions de servei públic, l'Administració estatal, amb les mateixes condicions descrites, podia també «intervenir la prestació» dels serveis de comunicacions electròniques.

Com es pot constatar, l'anterior article 4.6 LGTEL acotava expressament les potestats del Govern de l'Estat per remissió al que preveia la legislació en matèria de contractació administrativa. Per tant, hom podia pensar que la prerrogativa descrita tenia la seva raó de ser en l'àmbit dels contractes de gestió del servei públic, en els quals l'Administració pública manté la titularitat dels serveis afectats i els poders de policia necessaris per assegurar el seu bon funcionament i, per tant, en cas de la seva incorrecta prestació i d'acord amb els procediments i les garanties establerts a la llei, té la potestat de resoldre el contracte, rescatar-lo i assumir directament la seva gestió (art. 279.2 i 287.2 Reial decret legislatiu 3/2011).

Val a dir que el precedent article 4.5 LGTEL 2003, d'igual contingut que l'article 4.6 LGTEL 2014, abans d'ésser reformat pel RDL 14/2019, va ser impugnat pel Govern de la Generalitat davant la jurisdicció constitucional per raons competencials i que el Tribunal el va declarar ajustat al marc constitucional i estatutari. En síntesi, va considerar que el legislador estava

habilitat per dictar-lo a l'empara de les competències previstes a l'article 149.1.21 CE sobre règim general de telecomunicacions i que la intervenció de l'Estat, d'assumpció transitòria de la gestió directa de xarxes i serveis, estava determinada «por la necesidad de garantizar el servicio de telecomunicaciones en las situaciones acotadas por la norma», és a dir, «a los puros efectos de garantizar la prestación del servicio». En aquest sentit, va considerar que la norma no excloïa la intervenció de les comunitats autònomes que, en supòsits excepcionals i sempre que comptessin amb competències en matèria de seguretat o per a la prestació dels serveis públics afectats per l'anormal funcionament del servei o la xarxa, podien instar l'Estat perquè dugués a terme la dita intervenció (STC 72/2014, de 8 de maig, FJ 8). De manera semblant, en un posterior pronunciament, amb motiu de la norma que ara ens ocupa i efectuant un paral·lelisme amb l'argumentació llavors emprada, el Tribunal va recordar que la «asunción directa por el Estado de la prestación de servicios de comunicaciones por incumplimiento por los operadores de sus obligaciones de servicio público» està determinada per la «necesidad de garantizar el servicio de telecomunicaciones en las situaciones acotadas por la norma impugnada» (STC 20/2016, de 4 de febrer, FJ 8).

C) Arribats a aquest punt, convé ara examinar quins són els canvis principals que introdueix l'article 6.u RDL 14/2019 en l'apartat 6 de l'article 4 LGTEL.

A primera vista, s'observa que s'elimina la remissió que feia el redactat anterior a la legislació de contractes del sector públic. A més, el nou precepte, objecte de dictamen, amplia les potestats d'actuació de l'Administració estatal en la primera situació (quan es tracta de garantir la seguretat pública i la defensa nacional), ja que ara pot igualment assumir la gestió directa del servei, però també està facultat per dur a terme una «intervenció», sense que se n'especifiqui l'abast. D'altra banda, es redueix l'aparença del caràcter acotat de la mesura, eliminant els mots «certes» o

«determinades» per definir les xarxes i els serveis destinataris d'aquesta. Addicionalment, s'incrementen els pressupòsits que habilitarien l'actuació estatal: per una part, ja no es parla de «garantia» sinó d'«afectació» i, per l'altra, s'afegeixen els conceptes d'«ordre públic» i «seguretat nacional» i s'elimina el de «defensa nacional». A l'últim, s'incorpora un nou incís, tant per a la facultat estatal de gestió directa com d'intervenció, que declara que aquestes poden afectar «qualsevol infraestructura, recurs associat o element o nivell de la xarxa o del servei que sigui necessari per preservar o restablir l'odre públic, la seguretat pública i la seguretat nacional».

Pel que fa al segon incís de la versió anterior, amb la redacció donada pel Reial decret llei, es converteix en un nou paràgraf segons el qual la potestat «d'intervenir» recau sobre «els corresponents serveis» i «l'explotació de les corresponents xarxes», mentre que abans es projectava només sobre «la prestació dels serveis de comunicacions electròniques».

2. Un cop hem transcrit les distintes versions que ha adoptat l'article 4.6 LGTEL d'ençà de la seva aprovació inicial, ara ens pertoca analitzar la redacció que es correspon amb l'objecte del nostre Dictamen, és a dir, la que li dona l'article 6, apartat u, del Reial decret llei 14/2019.

El primer element que cal destacar de la norma és l'atribució d'una facultat general al Govern de l'Estat consistent en la capacitat per acordar la gestió directa o la intervenció de les xarxes i els serveis de comunicacions electròniques, en determinats supòsits, per tal de preservar i restablir l'ordre públic, la seguretat pública i la seguretat nacional (primer par. de l'art. 4.6 LGTEL). L'esmentat poder es configura, per part del mateix precepte, «amb caràcter excepcional i transitori», i amb un abast que pot «afectar qualsevol infraestructura, recurs associat o element o nivell de la xarxa o del servei que resulti necessari» per assolir l'objectiu previst.

Així doncs, es tracta d'un precepte inserit en un decret llei aprovat pel Govern de l'Estat, pel qual es modifica la Llei general de telecomunicacions, amb una finalitat i un contingut (pressupòsit i abast de l'actuació) que s'articulen al voltant de tres conceptes amplis que, de fet, són indeterminats, segons el criteri majoritari de la doctrina i, fins i tot, de la jurisprudència constitucional, com són el de l'ordre públic, la seguretat pública i la seguretat nacional.

La nostra anàlisi, d'acord també amb els dubtes expressats per la sol·licitud de dictamen, formulada pel Govern, es realitzarà des de dues vessants: d'una banda, respecte a l'habilitació competencial de l'Estat per efectuar la reforma de la LGTEL en els termes en què ho fa i, de l'altra, sobre l'eventual limitació de drets i llibertats fonamentals que pot comportar la mesura que s'hi preveu. Si bé el peticionari del nostre pronunciament situa les seves crítiques de manera prevalent en l'àmbit de les competències, segons es desprèn de la lletra del seu escrit, el cert és que quan fa esment de la manca d'autorització judicial per a l'activació de la capacitat d'actuació de l'Estat, està al·ludint en definitiva a l'esfera de les garanties dels drets fonamentals. Qüestió, aquesta darrera, que, segons la nostra opinió, és la que és susceptible de generar un examen més complex i amb més rellevància constitucional.

Així mateix, cal afegir, com a apunt metodològic de la nostra anàlisi, que restaria fora d'aquesta segona perspectiva la potestat de l'Administració estatal d'assumpció de la gestió directa de l'explotació de les xarxes i de la prestació dels serveis de comunicacions electròniques, que es troba acotada per la legislació de la contractació pública i que està prevista per als casos d'incompliment de les obligacions de servei públic definides a la mateixa Llei (par. segon del nou art. 4.6 LGTEL).

A) Com a primer assumpte, en la mesura que resulta important per a tots dos nivells de l'examen, plantejats per la sol·licitud, tractarem la possible competència de l'Estat per dur a terme aquesta regulació.

Sobre aquest aspecte, abans de res, i prenent com a base la descripció que acabem de realitzar respecte del contingut del nou article 4.6 LGTEL i els seus diversos paràgrafs, hem d'enquadrar-lo, des del punt de vista competencial, en la matèria de telecomunicacions en relació amb la seguretat pública. Aquesta classificació ens situa en els títols previstos als articles 149.1.21 i 149.1.29 CE, respectivament, i, en el cas primer, segons la jurisprudència del Tribunal Constitucional, en la matèria del règim general de les comunicacions, la qual té per objecte ordenar normativament i assegurar l'efectivitat de les comunicacions. Així, és competència de l'Estat el desplegament adequat de les xarxes com a base del servei i la regulació de les condicions per a la seva prestació i per a l'explotació d'aquestes, incloent-hi el règim jurídic dels operadors (entre d'altres, STC 72/2014, FJ 3).

En tots dos supòsits, el règim d'atribució de les capacitats és, amb caràcter general, el de l'exclusivitat en favor de l'Estat, tot i que amb determinades excepcions i particularitats que tot seguit indicarem. En ambdues matèries, el poder central compta amb una àmplia capacitat normativa, i en el nivell executiu la configuració és més complexa, especialment en el cas de la seguretat pública, i quan es tracta de les telecomunicacions disposa d'un plus afegit quan siguin necessàries per garantir la unitat o la uniformitat de les polítiques sectorials en el conjunt del territori de l'Estat (STC 20/2016, FJ 3).

Un cop assenyalat l'anterior, hem de remarcar que la competència del règim general de comunicacions inclou la regulació de les xarxes i els serveis de la comunicació electrònica i els recursos associats a uns i altres (infraestructures físiques, sistemes, dispositius, elements, etc.), com també la regulació i la garantia executiva, si s'escau, de l'accés i funcionament dels

serveis universals (en aquest sentit, STC 8/2012, de 18 de gener, FJ 7, i 20/2016, FJ 5).

Quant a les infraestructures i altres recursos per a la canalització i el desplegament de les xarxes de comunicacions electròniques, cal tenir en compte l'article 140.7 EAC, que atribueix a la Generalitat un feix de facultats executives en aquest àmbit material que, com a tals, no exclouen «que aquesta pugui realitzar altres competències de naturalesa similar, derivades […] de la posada en pràctica de la convergència tecnològica i la societat digital, així com de la necessitat de garantir la protecció de les xarxes i dels sistemes d'infraestructures que els donen suport» (DCGE 5/2017, de 29 de juny, FJ 3).

Pel que fa a la seguretat pública, l'Estat és el poder que compta amb la potestat legislativa en la matèria, amb el corresponent respecte al model singular de distribució de competències amb aquelles comunitats autònomes que es dotin d'un cos de policia propi. Com és evident i conegut, la Generalitat és la responsable del cos de Mossos d'Esquadra, i les competències de l'autogovern, en seguretat pública, estan recollides a l'article 164 EAC.

Segons aquest esquema competencial, en el cas de Catalunya es produeix una certa concurrència competencial en matèria de seguretat pública. D'una banda, l'Estat és el titular de la competència exclusiva de la seguretat pública, en els termes de l'article 149.1.29 CE i de la Llei orgànica 2/1986, i la Generalitat, en virtut de l'esmentat article 164 EAC, és competent en l'administració de la seguretat ciutadana en territori català, mitjançant el cos de Mossos d'Esquadra, la titularitat del qual també li atorga competències no només orgàniques sobre la policia sinó també funcionals i normatives en aquells àmbits connectats amb la funció policial, a més de les d'emergències

i protecció civil i seguretat privada establertes a l'article 132 i 163 EAC (per tots, DCGE 18/2015, de 26 de novembre, FJ 2).

Una vegada exposat en termes sintètics el model de distribució competencial, si el traslladem a l'examen del precepte que estem examinant, obtenim la següent conclusió: l'Estat és competent per legislar en l'àmbit material de les comunicacions electròniques i, en concret, en els supòsits en els quals aquest es connecta amb la seguretat pública, per raó, tal com hem indicat, de la seva doble competència *ex* article 149.1.21 i .29 CE. Així mateix, la seva capacitat no s'esgota en el nivell normatiu sinó que es pot estendre a la funció executiva, en aquest cas als supòsits excepcionals necessaris per garantir l'ordre públic, la seguretat pública i la seguretat nacional. Per precisar els termes, les condicions i els corresponents procediments d'aquests tres supòsits, cal tenir en compte les respectives lleis sectorials (per citar-ne algunes: Llei 36/2015, de 28 de setembre, de seguretat nacional; Llei 17/2015, de 9 de juliol, del Sistema Nacional de Protecció Civil; Llei 8/2011, de 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques; Reial decret de 14 de setembre de 1982, pel qual s'aprovà la Llei d'enjudiciament criminal (LECr); etc.)

Per tant, l'Estat, des d'un punt de vista del paràmetre de constitucionalitat i d'estatutarietat, està habilitat competencialment per legislar en la matèria del règim general de comunicacions (art. 149.1.21 CE) en relació amb la protecció de la seguretat pública (art. 149.1.29 CE), sens perjudici que ha de fer-ho respectant les competències de la Generalitat i el règim jurídic dels drets fonamentals protegits per la Constitució i susceptibles de ser afectats.

Quant a les capacitats de la Generalitat, ens podem remetre al DCGE 5/2017 (FJ 2 i 3), en el qual vam assenyalar que l'autogovern català incorpora les competències inherents al fet de disposar d'una policia pròpia, inclòs l'àmbit

de la investigació criminal en seu judicial, en la matèria de la protecció de l'espai de les comunicacions electròniques (ciberseguretat). Una competència concurrent, amb contingut normatiu orgànic i funcional, així com executiu, que es projecta amb especial intensitat en l'assegurament de les xarxes i els sistemes de l'Administració de la Generalitat i el seu sector públic i el sotmès al seu control per raó de les competències pròpies *ex* articles 140.7 i 164 EAC.

D'altra banda, i a tall d'informació addicional, com hem indicat anteriorment en aquest mateix fonament jurídic, la jurisprudència constitucional, que va analitzar aquesta qüestió competencial en relació amb l'article 4.5 LGTEL 2003 (STC 72/2014, FJ 8), va concloure que l'assumpció provisional i excepcional per part de l'Estat de la gestió directa dels serveis de telecomunicacions a fi de garantir el seu normal funcionament i que es compleixin les obligacions de servei públic que hi són inherents, no suposa el desplaçament de les competències autonòmiques sectorials que resultin afectades pels esmentats serveis (seguretat pública, protecció civil o sanitat).

Dit l'anterior, i atesa la configuració del precepte que estem examinant, és a dir, els termes en els quals està redactat, considerem que, a continuació, és procedent examinar-lo des de la perspectiva de la seva adequació al sistema dels drets fonamentals, en lloc de continuar l'exposició del paràmetre de constitucionalitat en relació amb la possible afectació de les competències de la Generalitat. El mateix fil argumental, que s'inicia tot seguit, aportarà les raons per les quals optem per aquest mètode d'anàlisi.

B) Seguidament, per tant, tractarem la qüestió relativa a la possible o potencial afectació de drets i llibertats fonamentals per part de l'article 6.u RDL 14/2019 (art. 4.6 LGTEL), principalment quant a l'article 18.3 CE, relatiu al dret al secret de les comunicacions i, així mateix, l'eventual incidència, per

la possible via de l'obstaculització o vulneració, d'una heterogeneïtat de drets i llibertats fonamentals com són la llibertat d'expressió i d'informació (art. 20 CE), el dret a la intimitat (art. 18.1 CE) o el dret a la protecció de dades (art. 18.4 CE), tal com veurem més endavant.

La raó de plantejar aquesta línia d'escrutini, a més dels retrets que fa la sol·licitud de dictamen, respon al motiu principal següent: la norma preveu una facultat governativa d'intervenció àmplia i d'abast general sobre el conjunt de les xarxes i els serveis de comunicacions electròniques, emparada en un seguit de conceptes jurídics indeterminats, com són l'ordre públic, la seguretat pública i la seguretat nacional, que configura un marc d'actuació administrativa susceptible d'afectar diversos drets fonamentals. I això és així en la mesura que l'accés a internet determina en gran part la viabilitat del seu exercici —aquest és el cas de la llibertat d'expressió i d'informació— i, alhora, atès que opera com a infraestructura i, fins i tot podríem dir en l'actualitat, com a condició de possibilitat de les comunicacions i de la transmissió de dades, amb la subsegüent i potencial afectació del dret formal al secret de les comunicacions i a la intimitat. En conseqüència, caldrà determinar si aquest esquema normatiu compleix les condicions i els requisits constitucionals i de la jurisprudència europea exigits a la legislació que té per objecte l'establiment de límits als drets i llibertats fonamentals.

La primera consideració que cal fer és la de l'objecte material sobre el qual es projecta la potencial capacitat d'actuació del Govern, és a dir, les xarxes i els serveis de comunicacions electròniques. Tal com ho hem descrit, en termes prolixos, en la primera part d'aquest fonament jurídic, la norma parteix d'una definició omnicomprensiva que, sintèticament, inclou els serveis de transport de senyals i els corresponents mitjans físics de transmissió, juntament amb els recursos i els serveis que hi estan associats i els donen suport, com ara les infraestructures, els sistemes, els dispositius, els equips, els terminals, les antenes, les construccions, els sistemes d'accés

condicional, les guies electròniques de programes o els serveis d'identitat, localització i presència. Aquesta expressió, doncs, agrupa el conjunt de mitjans i serveis que fan possible l'operativitat de les comunicacions telemàtiques, és a dir, tots aquells que incorporen algun element digital o informàtic i que caracteritzen la immensa majoria dels sistemes de comunicació actuals.

En paraules més sintètiques, podríem dir que es tracta d'internet i dels diferents nivells de connectivitat que aquesta xarxa global permet. Identificat l'anterior, és tan rellevant com evident assenyalar que actualment les comunicacions electròniques, de manera destacada internet, constitueixen la principal tecnologia en la qual es genera i circula la comunicació i la informació en la societat dels nostres dies. De fet, és tant decisiva la seva contribució que des de nombrosos sectors acadèmics, científics i també jurídics, les tecnologies de la comunicació electrònica, en les seves diferents modalitats, es consideren més un nou paradigma cultural, inclòs el seu vessant polític, que no pas un mer instrument o mitjà de comunicació més.

El Tribunal Constitucional, en els moments incipients d'un món encara emergent, ja indicava l'estret vincle entre la protecció de determinats drets fonamentals —el del secret de les comunicacions— en una «sociedad tecnológicamente avanzada» amb el «desarrollo cultural, científico y tecnológico colectivo» (STC 123/2002, de 20 de maig, FJ 5). Més endavant ja es parla d'un dret de nova generació a la protecció del propi entorn virtual, en el qual s'integraria tota la informació emmagatzemada massivament en format electrònic, ja sigui de manera conscient o inconscient, amb voluntarietat o sense, que va generant l'usuari, fins al punt de deixar un rastre susceptible de seguiment pels poders públics (STS 342/2013, de 17 d'abril, i 462/2019, de 14 d'octubre).

Igualment, la importància d'internet tant per a la comunicació humana com per al desenvolupament de la vida en societat ha estat recollida en altres àmbits, com ara en el si de les Nacions Unides, on el relator especial d'aquesta institució i un conjunt d'altes autoritats internacionals de llibertat d'expressió van emetre, l'1 de juny de 2011, la Declaració conjunta sobre llibertat d'expressió i internet, que, tot i que manca de valor normatiu, en el seu apartat 6 disposa que la interrupció (cancel·lació) de l'accés a internet o a una part d'aquesta, incloent-hi la reducció de la velocitat de navegació, aplicada a una població o a un segment d'aquesta, no es pot justificar en cap cas, ni tan sols per raó d'ordre públic o seguretat nacional. I, així mateix, que la negació d'accés a internet, a tall de sanció, constitueix una mesura extrema que s'ha d'adoptar per part de la justícia i sempre que no existeixin mesures menys restrictives, tenint en compte l'impacte que produeix en l'exercici dels drets humans. Aquesta Declaració ha estat confirmada recentment, el 10 de juliol de 2019, mitjançant la Declaració conjunta del vigèsim aniversari: Desafiaments per a la llibertat d'expressió en la propera dècada.

En conseqüència, la infraestructura i els serveis tecnològics, a la pràctica i en l'actual etapa de la civilització humana, han esdevingut una plataforma necessària i quasi bé indispensable per a la comunicació i, per tant, per a l'exercici de drets i llibertats de la importància de la llibertat d'expressió. En realitat, seria difícil identificar algun dret subjectiu, vinculat a la participació política en un sentit ampli, que no es vehiculés o relacionés, amb major o menor intensitat, amb les comunicacions electròniques.

La segona consideració estaria referida a l'abast funcional de la potestat atorgada a l'Administració de l'Estat, que la norma no precisa ni delimita. D'entrada, si acudim a la definició del concepte *intervenció*, segons el diccionari de la RAE, s'observa que les seves accepcions estan associades a les actuacions d'«Examinar y censurar las cuentas»; «Controlar o disponer

de una cuenta»; «Dicho de una autoridad: dirigir, limitar o suspender el libre ejercicio de actividades o funciones»; «Espiar, por mandato o autorización legal, una comunicación privada»; etc. D'altra banda, és un dels mots més emprats a la Llei d'enjudiciament criminal per qualificar les actuacions dels poders públics amb relació a la intercepció de les comunicacions en general (cap. IV i seg., títol VIII, llibre II, LECr).

Exposat l'anterior, podem arribar a una primera conclusió consistent en el fet que existeix una clara i estreta vinculació entre la garantia i l'exercici de determinats drets i llibertats fonamentals reconeguts a la Constitució i la gestió i intervenció de les xarxes i els serveis de comunicacions electròniques. De fet, més enllà del tractament constitucional i individualitzat, tots ells convergeixen en l'ús de les comunicacions electròniques, a les quals afecta de forma diversa en la mesura que aquestes són la via d'accés als continguts i a la societat de la informació: tot tipus de comunicacions telefòniques o telemàtiques, correus electrònics, serveis de missatgeria o xats en grup, tutelats per l'article 18.3 CE; contactes, fotografies i arxius personals, per l'article 18.1 CE; dades personals i de geolocalització, per l'article 18.4 CE; difusió d'idees i opinions, per l'article 20.1.*a* CE; emissió i recepció d'informació, per l'article 20.1.*d* CE; etc.

Els esmentats drets fonamentals han generat una nombrosa regulació i jurisprudència, tant pel que fa al seu assegurament i la seva garantia com en relació amb la seva ponderació respecte d'altres drets i béns jurídics susceptibles igualment de protecció. Aquí resulta impossible, per la seva extensió, reproduir-la en el seu conjunt, però sí que és apropiat i necessari per al nostre examen la citació de la doctrina general sobre la seva limitació per la via de la llei.

És àmpliament sabut que aquests drets fonamentals no són drets absoluts, i que poden ser sotmesos a limitacions en el marc d'un estat democràtic si es

compleixen determinats requisits i condicions. Aquesta configuració jurídica es troba recollida tant a la Constitució (art. 53.1 CE) com en les normes internacionals i europees que actuen com a paràmetre interpretatiu de l'ordenament estatal, segons l'article 10.1 CE: la Declaració universal de drets humans (1948), el Pacte internacional de drets civils i polítics (1966), el Conveni per a la protecció dels drets humans i de les llibertats fonamentals (1950) i la Carta de drets fonamentals de la Unió Europea (2001). En l'àmbit europeu és prou conegut que ha resultat especialment decisiva i determinant la jurisprudència emanada del Tribunal Europeu de Drets Humans.

D'acord amb el que acabem d'indicar, i de manera molt sintètica, els drets fonamentals poden ser limitats sempre que la seva restricció respongui a una finalitat legítima constitucionalment i necessària democràticament, es dugui a terme mitjançant una llei (reserva de llei) amb la qualitat normativa exigible per complir el principi de seguretat jurídica i es faci mitjançant mesures idònies, proporcionades, el menys lesives que es pugui i preservant un equilibri entre el dret i la limitació, de manera que el resultat de la constricció permeti un exercici raonable i el més ampli possible del dret o la llibertat que se sotmet a la regulació.

Quant a la finalitat perseguida, el Tribunal Europeu de Drets Humans ha acceptat com a finalitat legítima de la restricció dels drets i les llibertats dels individus, en termes generals, la preservació d'altres béns i valors dignes de protecció, com seria el cas de garantir la seguretat pública. Ara bé, exigeix en tot cas la «qualitat de la llei» que reguli la limitació, en el sentit que sigui accessible, clara i previsible. Així, la norma legal ha de definir les modalitats i l'extensió de l'exercici del poder atorgat amb la claredat suficient per aportar a l'individu destinatari una protecció adequada contra l'arbitrarietat dels poders públics. Addicionalment, s'han de poder preveure, en un grau raonable, segons les circumstàncies de cada cas, les conseqüències (les formalitats, condicions, restriccions o sancions) que es deriven de la seva

aplicació. I les limitacions s'han de fonamentar en una llei de singular precisió quan es tracta de procediments d'intercepció de les comunicacions, que constitueixen una intromissió a la vida privada i a la correspondència, de forma que és indispensable que les normes que els regulen siguin clares i detallades, encara més pel fet que la tecnologia disponible és cada vegada més sofisticada (STEDH 8691/79, de 2 d'agost de 1984, assumpte *Malone contra el Regne Unit*; 11105/84, de 21 d'abril de 1990, assumpte *Huvig contra França*; 11801/85, de 24 d'abril de 1990, assumpte *Kruslin contra França*).

En aplicació d'aquesta doctrina, en diverses ocasions s'han declarat contràries a l'article 8 CEDH les regulacions de la LECr sobre intervenció de les comunicacions telefòniques, perquè la llei no definia amb precisió la naturalesa de les infraccions que podien donar lloc a la dita intervenció ni les condicions per a la seva aplicació (STEDH 27671/95, de 30 de juliol de 1998, assumpte *Valenzuela Contreras contra Espanya*; 58496/00, de 18 de febrer de 2003, assumpte *Prado Bugallo contra Espanya*).

La manca d'algun dels elements determinants de la qualitat de la llei comporta la vulneració del dret afectat i, per tant, en aquests casos, el Tribunal Europeu ja no es pronuncia sobre la resta dels requisits necessaris perquè les ingerències o els límits al dret afectat siguin legítimes (si el límit és necessari en una societat democràtica per aconseguir un fi legítim i proporcional en relació amb aquest fi). A mode d'exemple, podem citar les STEDH ja esmentades dels assumptes *Kruslin contra França* i *Valenzuela Contreras contra Espanya*.

Per la seva part, el Tribunal Constitucional ha reiterat que tota ingerència estatal en l'àmbit dels drets fonamentals i les llibertats públiques, ja sigui perquè incideix directament en el seu desenvolupament (art. 81.1 CE) o perquè limita o condiciona el seu exercici (art. 53.1 CE), requereix una

habilitació legal (STC 49/1999, de 5 d'abril, FJ 4). Paral·lelament, ha destacat la importància que la mesura restrictiva estigui prevista en una norma legal que l'avali i que reuneixi les condicions mínimes que demanen les exigències de la seguretat jurídica i la certesa en el dret (art. 9.3 CE). En altres paraules, és un requisit «previo e insoslayable» l'existència d'una cobertura legal expressa i clara de la ingerència, que defineixi les modalitats i l'extensió de l'exercici del poder atorgat amb la suficient claredat per aportar a l'individu una protecció adequada contra l'arbitrarietat (STC 84/2018, de 16 de juliol, FJ 2 i 3, fent cita de la STC 217/2015, de 22 d'octubre, FJ 2).

Així, considera que és insuficient, des de la perspectiva de la qualitat de la llei, l'habilitació genèrica que no preveu els pressupòsits, les condicions i la durada màxima de la intervenció (STC 169/2001, de 16 de juliol, FJ 6 i 8), com també ho és la que suscita una indeterminació sobre els casos als quals s'aplica la restricció, defecte que impedeix el compliment de la seva funció de garantia i que, per contra, atorga el control de la restricció a la lliure voluntat de qui l'executa (STC 292/2000, de 30 de novembre, FJ 15, i 76/2019, de 22 de maig, FJ 5).

Igualment, aquest Consell, en el DCGE 7/2015, de 4 de juny, en relació amb l'obligació que les mesures que limiten drets fonamentals han d'estar previstes a la llei i, alhora, han de reunir certes exigències de «qualitat», vàrem dir que «la norma ha de ser suficientment clara i ha de permetre preveure, en un grau raonable segons les circumstàncies de cada cas, les conseqüències que deriven de la seva aplicació. Per altra part, el grau de precisió depèn en gran mesura del contingut i de l'àmbit d'aplicació de la restricció, així com també dels seus destinataris. De la mateixa manera, la noció de previsibilitat s'aplica, no només a un comportament respecte del qual qualsevol ciutadà pugui preveure les conseqüències que se'n deriven, sinó també a les formalitats, condicions, restriccions» (FJ 4).

Arribats a aquest punt, cal insistir que el requisit de qualitat en la llei s'ha de complir sempre que es vulgui restringir legítimament l'exercici d'un dret fonamental, i això sens perjudici que en alguns supòsits, com és el cas del secret de les comunicacions, es parteixi, per mandat constitucional (art. 18.3 CE), d'un nivell de protecció més alt, atès que és necessària una autorització judicial prèvia per a la intervenció del seu exercici. Val a dir, però, que el Tribunal Constitucional, invocant el dret a la intimitat per atorgar protecció constitucional al cúmul d'informació personal derivada de l'ús dels instruments tecnològics (art. 18.1 CE), ha declarat que la regla general també hauria de ser la limitació d'aquest dret mitjançant resolució judicial motivada. Ara bé, atès que no hi ha reserva constitucional en aquest sentit, ha admès que la llei autoritzi la limitació dels drets i llibertats sempre que aquesta es dugui a terme respectant els principis de proporcionalitat i de raonabilitat. Exigeix, per tant, l'estricta observança del principi de proporcionalitat de la mesura restrictiva, en les seves tres dimensions: judici d'idoneïtat (si la mesura permet assolir l'objectiu proposat i és congruent amb aquest); judici de necessitat (si no existeix una altra mesura més moderada i de menor intensitat coactiva per a la consecució de la finalitat amb igual eficàcia); judici de proporcionalitat en sentit estricte (si la mesura és ponderada o equilibrada, de manera que en deriven més avantatges o beneficis per a l'interès general que perjudicis sobre altres béns o valors en conflicte) (per totes, STC 173/2011, de 7 de novembre, FJ 2, i en el mateix sentit, DCGE 7/2015, de 4 de juny, FJ 3, i 2/2019, de 22 de febrer, FJ 3).

C) Una vegada hem exposat breument el paràmetre de limitació dels drets fonamentals, hem de projectar-lo sobre la norma que és objecte del nostre Dictamen. En primer lloc, examinarem la finalitat del precepte; analitzarem el sentit i l'abast del seu contingut a fi de determinar si pot afectar il·legítimament l'exercici de drets fonamentals, i, segons el resultat, ens pronunciarem sobre la seva adequació a la Constitució.

Respecte de la finalitat, si ubiquem el precepte en el si de la norma legal en la qual s'insereix la Llei general de telecomunicacions i, alhora, tenim en compte també la seva intitulació i el seu contingut regulador, resulta clar, com hem vist àmpliament en l'inici d'aquest fonament jurídic, que es tracta d'un supòsit en el qual concorren les matèries de règim general de les comunicacions i de seguretat pública, en un sentit ampli (ordre públic i seguretat nacional).

Amb relació a l'ordre públic, la seguretat pública i la seguretat nacional hem de formular les següents consideracions:

L'*ordre públic* és un concepte jurídic indeterminat, amb origen i apogeu en la governança espanyola del segle XIX i de l'etapa de la dictadura franquista, que amb l'entrada en vigor del nou règim constitucional va perdre bona part del seu sentit tradicional en la mesura que aquest esdevenia incompatible amb les garanties constitucionals pròpies d'una democràcia. D'aquesta manera, l'ordre públic passà de la vella i obsoleta construcció com a clàusula preventiva i repressiva d'intervenció governativa, orientada a la restricció de drets i llibertats, especialment els de naturalesa política, cap a una noció actualitzada i més acotada denominada *seguretat pública*. Així, la norma fonamental de 1978 abandonà l'ús legislatiu anterior, fins al punt que únicament el preveu de forma explícita en tres ocasions i en uns termes ben diferents: com a límit al dret de reunió i manifestació (art. 21.2 CE) i a l'exercici de la llibertat religiosa en espais públics (art. 16.1 CE), per assegurar el respecte simultani a d'altres drets i com a bé jurídic susceptible de ser protegit mitjançant la funció de la seguretat ciutadana, que és exercida de manera principal per les forces i els cossos de seguretat (art. 104 CE). Dit d'una altra manera, l'ordre públic en l'estat de dret actual és concebut com aquell bé, o altrament dit valor o espai de tranquil·litat i de convivència social, que actua com a condició necessària per a l'exercici d'altres drets fonamentals i llibertats públiques.

El mencionat canvi de paradigma jurídic ja va ser fixat per la jurisprudència incipient del Tribunal Constitucional (STC 33/1982, de 8 de juny, FJ 3), que va establir que el concepte de seguretat pública era una noció més precisa i pròpia del nou sistema constitucional, de forma que l'ordre públic restava circumscrit als aspectes damunt indicats. Des d'aquella època, ja llunyana, el cert és que el Tribunal no ha desenvolupat una posterior doctrina delimitativa de l'ordre públic, quant al seu contingut i els seus contorns, i el mateix podríem dir de la doctrina del Tribunal Europeu de Drets Humans. Aquest darrer, més enllà d'acceptar, segons una anàlisi ponderada, cas per cas, la validesa d'aquest concepte jurídic indeterminat com a límit legítim a l'exercici de certs drets fonamentals, sí que ha recordat que l'ordre públic no pot ser utilitzat per la legislació dels estats de manera excessivament expansiva fins al punt d'esdevenir un instrument de restricció o d'obstaculització de les llibertats i els drets fonamentals, especialment en l'esfera de la llibertat d'expressió i els drets de participació política, en un sentit ampli (amb un èmfasi destacat en els drets de reunió, associació i manifestació, i de dissidència en general: STEDH 31684/05, de 5 de març de 2009, assumpte *Barraco contra França*; 17843/11, de 16 de gener de 2018, *assumpte Dinçer contra Turquia*; 11798/85, de 23 d'abril de 1992, assumpte *Castells contra Espanya*, entre d'altres). En tot cas, si procedim a dur a terme una certa destil·lació de la seva doctrina, obtindríem el principi que l'ordre públic és legítim per garantir l'absència de violència, en un context d'existència d'un risc cert, clar i imminent en què aquesta es pot arribar a desencadenar.

En conseqüència, a tall de resum, podem sostenir que, tot i que es tracta d'un concepte jurídic indeterminat, la previsió de l'ordre públic en les lleis és legítima si té per objecte prevenir i combatre un supòsit clar d'afectació de la pau i de la convivència social. Tanmateix, la seva invocació per part del legislador ha de ser restrictiva i respectuosa amb l'exercici dels drets fonamentals i de les llibertats, de manera que no n'obstaculitzi ni en

desincentivi la pràctica, condició que requereix una tècnica precisa i clara en la seva regulació, tant pel que fa a la concreció dels supòsits habilitants per a la seva activació com en relació amb les condicions i la previsibilitat del seu ús per part dels poders públics.

Quant a la *seguretat pública*, com acabem d'exposar, emergeix com a nou concepte amb la Constitució de 1978, i es configura com a matèria de distribució competencial, en aquest cas en règim d'atribució exclusiva a l'Estat *ex* article 149.1.29 CE i amb la participació destacable de les comunitats autònomes que es dotin de policia pròpia, essent un dels dos casos més rellevants el català, i alhora com a bé jurídic que garanteix la tranquil·litat ciutadana, principalment a través de la seguretat ciutadana i la protecció civil. La jurisprudència constitucional en seguretat pública ha resultat molt més extensa que en el cas de l'ordre públic, i ha estat dictada sobretot en supòsits de conflictivitat competencial o en l'examen de constitucionalitat de les lleis sectorials de capçalera de les esmentades submatèries (Llei orgànica 4/2015, de 30 de març, de protecció de la seguretat ciutadana i Llei 17/2015, de 9 de juliol, del Sistema Nacional de Protecció Civil). A tall de resum, podríem dir que l'alt tribunal ha equiparat en gran mesura la seguretat pública a l'activitat funcional i orgànica orientada a la protecció de les persones i els béns i, per tal de limitar el seu potencial expansiu, ha tendit a vincular-la, tot i que sense excloure altres espais materials connexos, amb l'esfera de les funcions que despleguen els cossos de seguretat i de prevenció i reacció en les emergències (entre d'altres, STC 58/2017, d'11 de maig, FJ 3 i 4; 87/2016, de 28 d'abril, FJ 5; 86/2014, de 29 de maig, FJ 2 a 4).

Darrerament, però, l'abast de la seguretat pública s'ha ampliat en dos nous àmbits d'actuació que fins l'any 2015 eren inèdits, com a mínim pel que fa a la seva explicitació formal i al fet de disposar d'una legislació sectorial pròpia: ens estem referint a la seguretat nacional i a la ciberseguretat. En

sengles sentències recents, el Tribunal Constitucional ha optat per no considerar-los una competència nova sinó que els ha reconduït i subsumit, en bona part, en la seguretat pública. En el cas de la seguretat nacional hi ha fet concórrer, junt amb la seguretat pública, la matèria de la defensa (STC 184/2016, de 3 de novembre, FJ 3), i en el supòsit de la ciberseguretat, ha establert el vincle amb les competències de telecomunicacions i de la seguretat nacional (STC 142/2018, de 20 de desembre, FJ 4 a 6).

Respecte a aquesta última, i atesa la seva evident connexió amb el present Dictamen, creiem oportú reproduir el següent raonament:

> «En suma, puede afirmarse que la evolución de las tecnologías de la información y de la comunicación ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo de las actividades económicas y sociales. Prueba de ello es que los operadores de redes y servicios de comunicaciones electrónicas disponibles al público están obligados a gestionar "adecuadamente los riesgos de seguridad que puedan afectar a sus redes y servicios a fin de garantizar un adecuado nivel de seguridad y evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en las redes interconectadas" (art. 44.1 de la Ley 9/2014, de 9 de mayo, general de telecomunicaciones). Atendiendo a lo que se ha expuesto, puede concluirse que la ciberseguridad se incluye en materias de competencia estatal en cuanto, al referirse a las necesarias acciones de prevención, detección y respuesta frente a las ciberamenazas, afecta a cuestiones relacionadas con la seguridad pública y la defensa, las infraestructuras, redes y sistemas y el régimen en general de telecomunicaciones.» (FJ 4)

Així, d'acord amb el que hem exposat, es pot concloure que els conceptes d'ordre públic, seguretat pública i seguretat nacional, amb les corresponents modulacions, són conceptes interconnectats, susceptibles de legitimar la

intervenció de l'Estat en situacions de risc per a les persones i els béns, en l'amplíssim ventall d'àmbits en els quals es projecta l'espai públic, inclòs el tecnològic, i els quals en tot cas es caracteritzen pel seu contingut indeterminat, amb el subsegüent marge d'apreciació i discrecionalitat quant als límits de la intervenció i, per tant, també en la seva potencial capacitat d'afectar l'exercici de drets i llibertats individuals. Respecte de l'esmentada configuració, cal afegir, per completar la síntesi, que la jurisprudència dels més alts tribunals en la interpretació dels drets constitucionals tampoc no els ha precisat ni acotat més enllà de vincular-los, cas per cas, a la protecció i la tranquil·litat ciutadana, a la necessitat de preservar l'ordre pacífic i no violent i, en conseqüència, els ha identificat amb el vessant orgànic i funcional dels serveis públics de policia i d'emergències.

Tanmateix, tant el Tribunal Constitucional com el Tribunal Europeu de Drets Humans han establert la necessitat que la seva regulació com a límits per a l'exercici dels drets i les llibertats dels ciutadans sigui per llei, respongui a una necessitat democràtica i es formuli en termes acotats i el menys constrictius possible, i que la seva aplicació es dugui a terme amb la intensitat mínima i proporcionada, de manera que el resultat els dificulti o els restringeixi el menys possible.

Tornant a l'examen de la norma que ens ocupa, el nou redactat de l'article 4.6 LGTEL que reforma el Reial decret llei s'articula al voltant d'aquests tres conceptes que operen com a finalitat o objectiu de la norma: la preservació o restabliment de l'ordre públic, la seguretat pública i la seguretat nacional, i, al mateix temps, els preveu com a supòsits d'aplicació o habilitants per a l'activació de la facultat d'intervenció del Govern de l'Estat.

D'entrada, aquesta conformació normativa contribueix a generar un marc molt ampli i, fins i tot, imprevisible respecte del seu règim d'aplicació: es recorre a tres conceptes jurídics indeterminats per justificar l'atribució del

poder al Govern, sense necessitat d'autorització judicial i ni tan sols cap requisit procedimental administratiu específic per intervenir el conjunt de les xarxes i els serveis, els quals simultàniament són establerts com a objectiu i pressupòsit habilitant.

Es tracta d'una construcció tan imprecisa i difosa que contrasta amb la regulació de la legislació processal penal actualment vigent per a la intervenció de les comunicacions personals en supòsits d'investigació policial i penal. La comparació que realitzem a continuació és rellevant perquè es tracta del supòsit més destacat del qual disposa l'ordenament jurídic quant a la intervenció de comunicacions per part dels poders públics, susceptible d'afectar l'exercici dels drets fonamentals *ex* article 18.3 CE, i el qual ha estat sotmès a una intensa i recurrent tasca d'escrutini per part dels tribunals (Tribunal Suprem, Tribunal Constitucional i Tribunal Europeu de Drets Humans). En aquest sentit, és important recordar que el cas del dret al secret de les comunicacions es tracta d'un dret essencialment formal, que és vulnerat pel mer fet de la intercepció il·legítima, al marge o a banda dels continguts de la comunicació. Així, els articles 588 bis.*a* a 588 *octies* LECr, després de diverses sentències contràries a l'Estat espanyol per part del Tribunal Europeu de Drets Humans, estableixen un seguit de requisits concrets previs a l'autorització judicial que ha de donar lloc a la intercepció d'una comunicació, ja sigui de naturalesa privada o pública.

En primer lloc, la llei processal exigeix que els indicis delictuosos que justifiquin la sol·licitud es refereixin a tipus penals amb penes superiors als tres anys, a delictes comesos en el si d'un grup o una organització criminal, o que es tracti de delictes de terrorisme. Tot seguit, correspon al jutge la decisió de la intervenció, segons l'imperatiu constitucional consignat a l'article 18.3 CE, darrer incís, el qual l'adoptarà només si escau i en uns termes acotats d'acord amb els principis d'especialitat, idoneïtat, excepcionalitat, necessitat i proporcionalitat de la mesura.

Si retornem al precepte que estem examinant (art. 6.u RDL 14/2019), també es pot comprovar que es projecta sobre el conjunt de les xarxes i els serveis de comunicacions electròniques amb un potencial d'intervenció integral i quasi il·limitat. Així es desprèn de manera immediata de la literalitat del text:

> «6. El Govern, amb caràcter excepcional i transitori, pot acordar l'assumpció per l'Administració General de l'Estat de la gestió directa o la intervenció de les xarxes i els serveis de comunicacions electròniques en determinats supòsits excepcionals que puguin afectar l'ordre públic, la seguretat pública i la seguretat nacional. En concret, aquesta facultat excepcional i transitòria de gestió directa o intervenció pot afectar qualsevol infraestructura, recurs associat o element o nivell de la xarxa o del servei que sigui necessari per preservar o restablir l'ordre públic, la seguretat pública i la seguretat nacional.»

La combinació de l'atribució d'una enorme discrecionalitat al Govern de l'Estat a l'hora d'activar la intervenció de les comunicacions electròniques, el seu caràcter potencialment omnicomprensiu sobre el conjunt de la xarxa i els serveis en què pot operar, junt amb l'absència de previsió de qualsevol mena de delimitació funcional, de procediment específic o de garantia addicional quant als continguts i els subjectes susceptibles de ser afectats per la intervenció, converteixen aquest precepte en una veritable clàusula genèrica d'intervenció governamental.

L'eventual refutació a l'afirmació que acabem de sostenir, que consistiria a asseverar que la capacitat del Govern de l'Estat només afectaria el suport instrumental de les comunicacions, és a dir, les infraestructures físiques o tècniques (cablejat, servidors, antenes, etc.), i no els continguts ni la informació, els quals restarien preservats de l'afectació administrativa, així com el raonament que tan sols s'intervindrien amb una finalitat de restabliment del servei universal en supòsits de caiguda del sistema (cosa

que ja està prevista expressament en un altre paràgraf del mateix precepte), nosaltres considerem que no és ni de bon tros la interpretació que es desprèn de manera immediata, natural i raonable de la literalitat del text. I, en el cas que fos així, ni que sigui en part, tampoc foragita la potencial afectació que implica per a l'exercici de determinats drets, com la llibertat d'expressió, el bloqueig, la interrupció o l'obstaculització de l'accés universal a la xarxa per la qual circula la informació i la comunicació.

Creiem important insistir en el fet que el text del primer paràgraf de l'article 4.6 LGTEL opera en termes tan genèrics i indeterminats que esdevenen incompatibles amb una regulació garant dels drets fonamentals. Respecte del concepte «intervenció», aquest dona cabuda a una potencial actuació tan àmplia com imprecisa pel que fa a la seva predeterminació o previsibilitat; interpretació que es reforça quan el precepte no es limita a indicar una finalitat reparadora (el restabliment de l'ordre públic, la seguretat pública o la seguretat nacional) un cop s'ha produït un dany o un risc de dany imminent i cert sinó que també dona cobertura a una actuació preventiva («en determinats supòsits excepcionals que puguin afectar l'ordre públic, la seguretat pública i la seguretat nacional»).

Aquesta configuració, segons el nostre parer, apuntala la interpretació de la clàusula genèrica i imprevisible. Defectes, aquests, en la qualitat normativa de l'article 6, apartat u, RDL 14/2019 que també es reflecteixen en la justificació vaporosa i inaprehensible del preàmbul. Així, amb caràcter general es diu que:

> «Els recents i greus esdeveniments succeïts en part del territori espanyol han posat de relleu la necessitat de modificar el marc legislatiu vigent per fer front a la situació. Aquests fets demanen una resposta immediata per evitar que es reprodueixin successos d'aquesta índole amb l'establiment d'un marc preventiu amb aquesta finalitat, l'objectiu últim de la qual sigui protegir els

> drets i les llibertats reconeguts constitucionalment i garantir la seguretat pública de tots els ciutadans.» (apt. I, par. sisè)

O també que:

> «Com s'ha justificat als apartats anteriors, les mesures que conté aquest Reial decret llei tenen com a finalitat incrementar l'estàndard de protecció de la seguretat pública davant les amenaces creixents que planteja l'ús de les noves tecnologies i sempre en vista dels últims successos en territori espanyol.» (apt. VI, par. cinquè)

I, més concretament, respecte al precepte que ara s'analitza:

> «Així, en concret, es modifiquen els articles 4.6 i 6.3 de la Llei 9/2014, de 9 de maig, per reforçar les potestats del Ministeri d'Economia i Empresa per portar a terme un control més gran i per millorar les seves possibilitats d'actuació quan la comissió d'una presumpta actuació infractora a través de l'ús de les xarxes i els serveis de comunicacions electròniques pugui suposar una amenaça greu i immediata per a l'ordre públic, la seguretat pública o la seguretat nacional o quan en determinats supòsits excepcionals que també puguin comprometre l'ordre públic, la seguretat pública i la seguretat nacional sigui necessària l'assumpció de la gestió directa o la intervenció de les xarxes i els serveis de comunicacions electròniques.» (apt. II, par. vint-i-sisè)

Així, la reforma que opera el Reial decret llei en la LGTEL, segons les paraules mateixes del legislador, confirmaria la tesi de l'evolució de la finalitat i l'objecte del precepte, ja que la justificació del preàmbul, la desvinculació de la llei de contractes públics i els canvis subtils però significatius de la seva literalitat evidencien la seva col·lisió amb la intenció originària de la Llei, la qual havia de ser interpretada d'acord amb els principis de l'article 5 LGTEL i que, per contra, en la seva versió actual es manifesta amb substantiva disconformitat amb aquests principis.

D'acord amb l'anterior, podem arribar a la conclusió que, tot i que la nova redacció de l'article 4.6 LGTEL (segons la versió del Reial decret llei) ha variat en pocs i limitats aspectes respecte de la redacció de la Llei general de telecomunicacions (en la seva versió de l'any 2014), en realitat el seu objecte i la seva finalitat han mutat de manera substantiva fins al punt que l'actual redactat és incompatible no només amb el principi de seguretat jurídica *ex* article 9.3 CE, sinó també quant a una adequada garantia constitucional de les condicions per a l'exercici de determinats drets fonamentals.

Si desenvolupem l'argument anterior, podem precisar que el seu text genera un greu marc d'imprevisibilitat donat el caràcter amplíssim i indeterminat de la casuística que hi pot trobar cabuda, ni que sigui formalment, sota el paraigua de conceptes com el de l'ordre públic, la seguretat pública o la seguretat nacional. Hipòtesi, aquesta, que és confirmada pel mateix preàmbul quan es manifesta incapaç de concretar els motius que justifiquen la reforma d'aquest precepte més enllà de les referències eufemístiques i velades que apunta respecte a les amenaces de les noves tecnologies i als conflictes o aldarulls succeïts recentment a «part del territori espanyol» i que justificarien per raons d'urgència i seguretat l'aprovació del Reial decret llei on es conté la reforma en qüestió.

Des de la perspectiva de les condicions per a l'exercici de determinats drets fonamentals, la indefinició i la indeterminació del precepte encara esdevé més greu. Els pressupòsits habilitants, així com l'abast de la intervenció, obren un espai d'amplíssima discrecionalitat administrativa, pel que fa al *quan* i al *què*, els supòsits concrets de l'activació i l'objecte material sobre el qual es pot projectar, però també en relació amb el *com*, amb una evident indeterminació funcional quant a les mesures limitatives que pot emparar. Així, resta a la lliure apreciació del Govern estatal una facultat d'intervenció

que al capdamunt no requereix ni d'un procediment específic mínimament articulat (en contrast, per exemple, amb el cas de la Llei de seguretat nacional) ni de l'autorització judicial. En un marc com aquest, s'obren espais a l'aplicació de la norma lesius, tant pel que fa a la llibertat d'expressió i d'informació (amb la xarxa intervinguda per l'acció governamental no es donen les condicions per al seu lliure i complet exercici) com de potencial afectació respecte del secret de les comunicacions, la intimitat i la deguda protecció de les dades.

Quant a aquests darrers drets fonamentals, no ho hem d'oblidar i aquí esdevé cabdal recordar-ho, avui en dia les xarxes i els serveis de comunicacions electròniques són molt més que una mera infraestructura o una tecnologia per a la comunicació, fins al punt que han esdevingut autèntiques condicions de possibilitat o bàsiques per a l'exercici dels precitats drets fonamentals, veritables pilars de les societats democràtiques i plurals. El mateix Tribunal Europeu de Drets Humans, en la decisió de l'assumpte *Ahmet Yildirim contra Turquia,* STEDH 3111/10, de 18 de desembre de 2012, resultant definitiva el 18 de març de 2013, ja va indicar amb motiu d'una restricció governamental d'accés a internet que, ni que fos limitada, suposava una vulneració dels drets del Conveni europeu per a la protecció dels drets humans i les llibertats fonamentals en la mesura que «Internet es en la actualidad el principal medio de la gente para ejercer su derecho a la libertad de expresión y de información: se encuentran herramientas esenciales de participación en actividades y debates relativos a cuestiones políticas o de interés público» (apt. 54). En la nostra era, la distinció tradicional entre instrument i contingut en determinats casos, i en concret en l'àmbit de les noves tecnologies i el dret o el contingut que aquest pretén garantir, ha acabat diluint-se i ha esdevingut més un artifici conceptual, fruit de la pervivència de les classificacions acadèmiques i intel·lectuals dels segles XIX i XX, que no pas una realitat, ja no incipient sinó consolidada, en la qual sovint l'instrument determina i, fins i tot, crea el contingut.

Dit això, convé ara recuperar la ja exposada doctrina del Tribunal Constitucional, a través de la STC 169/2001, la qual, acollint el criteri encetat per la STC 27/1981, de 20 de juliol (FJ 10) i reflectit a la STC 49/1999, de 5 d'abril (FJ 4), argumenta que «la legitimidad constitucional de cualquier injerencia del poder público en los derechos fundamentales requiere que haya sido autorizada o habilitada por una disposición con rango de Ley, y que la norma legal habilitadora de la injerencia reúna las condiciones mínimas suficientes requeridas por las exigencias de seguridad jurídica y certeza del derecho».

En el mateix sentit, i de fet amb motiu de diversos assumptes en els quals ha estat part el mateix Estat espanyol, la doctrina del Tribunal Europeu de Drets Humans ha establert reiteradament que una llei que tingui per objecte la limitació d'un dret fonamental, com seria el cas dels previstos als articles 18 (intimitat i secret de les comunicacions) i 21 (dret de reunió i d'associació), a banda dels ja esmentats criteris de la legitimitat de la finalitat i de la necessitat democràtica de la mesura i la subsegüent proporcionalitat de la regulació, ha de complir, abans de res, una primera condició vinculada a la reserva de llei, que és, precisament, la seva qualitat normativa, connectada al principi de seguretat jurídica, és a dir, a la previsibilitat. I aquesta propietat o atribut s'identifica amb una regulació prou específica i detallada per evitar un marge d'apreciació dels poders públics, a l'hora d'actuar restringint els drets afectats, que pugui esdevenir il·limitat o molt ampli. Així, la característica de la nitidesa i la claredat en l'abast, les condicions habilitants per al seu exercici i els termes i límits de l'activitat constrictiva són elements cabdals en la valoració de la validesa i legitimitat de la norma segons les prescripcions del Conveni europeu per a la protecció dels drets humans i les llibertats fonamentals.

Aquest cànon s'ha de complir amb especial cura quan la mateixa llei no preveu la intervenció judicial en el procés de limitació governativa o administrativa dels drets, i de manera encara més exigent en actuacions dels poders públics que poden ser de tipus preventiu o anticipatori, sota l'empara del supòsit legal de «la imperiosa necessitat» de prevenir un potencial dany o fer front a un «risc clar immediat» en les persones i els béns.

D'acord amb tot l'anterior, podem concloure que la regulació examinada, el primer paràgraf de l'apartat 6 de l'article 4 LGTEL, no respecta els estàndards mínims de qualitat normativa que exigeixen tant la jurisprudència del Tribunal Constitucional com la del Tribunal Europeu de Drets Humans. I això és així perquè, tal com ho hem raonat, el precepte es configura sobre una finalitat, uns supòsits habilitants i un procediment que el converteixen en una regulació mancada de la previsibilitat necessària que s'exigeix a una llei que és susceptible de constrènyer drets fonamentals protegits pel Conveni europeu de drets humans i la Constitució. Així, no compleix el primer requisit de validesa exigible a aquest tipus de legislació, la qual, a més, tot sigui dit a l'efecte de completar el test de validesa, un cop assolida la mínima qualitat normativa, hauria d'acreditar també la seva legítima necessitat per a un estat democràtic, la seva idoneïtat pel que fa al contingut de la mesura, a més de la proporcionalitat en el seu conjunt a l'hora de garantir l'equilibri entre la restricció i la viabilitat de l'exercici del dret o drets afectats. Aquests darrers elements, però, tot i que han estat apuntats, ja no seran examinats respecte de la norma que ens ocupa, atès que la primera condició de validesa, la qualitat de la llei, com acabem de raonar, s'incompleix.

Dels raonaments tot just exposats es desprèn que l'apartat 6 de l'article 4 de la Llei 9/2014, de 9 de maig, general de telecomunicacions, en la seva nova redacció, vulnera l'article 9.3 CE, quant a les exigències de qualitat de la llei per legitimar la ingerència dels poders públics en els drets fonamentals i les llibertats públiques, i alhora també és contrari a la jurisprudència del Tribunal

Europeu de Drets Humans, de rellevància constitucional a través de l'article 10.1 CE, relativa a la qualitat de les lleis susceptibles d'afectar els drets i les llibertats del Conveni europeu.

Per tant, hem de concloure que l'apartat u de l'article 6 RDL 14/2019, de 31 d'octubre, 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» administrativa estatal, és inconstitucional perquè vulnera l'article 9.3 CE.

Finalment, ens correspon realitzar una darrera observació sobre la qüestió competencial, que hem indicat a l'inici del present fonament jurídic i que hem deixat inconclusa atès que hem passat a tractar el vessant relacionat amb l'afectació de drets fonamentals. I, arribats a aquest punt, considerem que no es pot reprendre la tasca orientada a obtenir una conclusió sobre l'eventual vulneració de les competències de la Generalitat perquè, com acabem d'exposar, la manca de qualitat normativa impedeix identificar amb precisió l'abast i els límits de la potencial intervenció administrativa i governamental per part de l'Estat. Condició que esdevé imprescindible per poder procedir a l'examen de la delimitació de funcions i responsabilitats entre les administracions que són titulars de competències concurrents en les matèries objecte de la norma. És a dir, la insuficient precisió i la imprevisibilitat del tenor literal del precepte deixen sense sentit dur a terme l'operació jurídica de la delimitació de competències segons els termes del seu redactat per causa de la inconstitucionalitat ja apreciada, però també per la manca de la definició mínima exigible per poder fer-ho.

3. A continuació, ens pertoca pronunciar-nos sobre l'apartat 5 de l'article 6 RDL 14/2109, pel qual es reformula l'apartat 1 de l'article 81 LGTEL i al qual es dona la redacció següent:

> «1. Prèviament a l'inici del procediment sancionador, l'òrgan competent del Ministeri d'Economia i Empresa pot ordenar, mitjançant una resolució sense audiència prèvia, el cessament de la presumpta activitat infractora quan hi hagi raons d'urgència imperiosa basada en un dels supòsits següents:
> a) Quan hi hagi una amenaça immediata i greu per a l'ordre públic, la seguretat pública o la seguretat nacional.
> b) Quan hi hagi una amenaça immediata i greu per a la salut pública.
> c) Quan la suposada activitat infractora pugui ocasionar perjudicis greus al funcionament dels serveis de seguretat pública, protecció civil i d'emergències.
> d) Quan s'interfereixi greument en altres serveis o xarxes de comunicacions electròniques.
> e) Quan creï greus problemes econòmics o operatius a altres proveïdors o usuaris de xarxes o serveis de comunicacions electròniques o altres usuaris de l'espectre radioelèctric.»

Com es desprèn del seu contingut, el precepte objecte de dictamen, inserit en el cos normatiu de la Llei general de telecomunicacions sobre la inspecció i llur règim sancionador, regula les «Mesures prèvies al procediment sancionador». En concret, atribueix a un òrgan de l'Administració de l'Estat (el Ministeri d'Economia i Empresa) la potestat per ordenar, abans que s'iniciï el procediment sancionador i mitjançant una resolució sense audiència prèvia, quan existeixin raons d'imperiosa urgència, el cessament de la presumpta activitat infractora. Aquesta urgència s'ha de projectar sobre un dels cinc supòsits que s'han transcrit abans, tots recollits per l'article 81.1: quan existeixi una amenaça immediata i greu per a l'ordre públic, la seguretat pública, la seguretat nacional o la salut pública (lletres *a* i *b*); quan es puguin produir perjudicis greus per al funcionament dels serveis de seguretat pública, protecció civil i emergències com a conseqüència de l'activitat infractora (lletra *c*); quan s'interfereixi greument en altres serveis o xarxes de comunicacions electròniques (lletra *d*), i quan aquesta activitat creï greus problemes econòmics o operatius per a altres proveïdors o usuaris de

xarxes o serveis de comunicacions electròniques o els restants usuaris de l'espectre radioelèctric (lletra *e*).

Amb la finalitat d'obtenir la corresponent conclusió, en primer lloc, descriurem la caracterització del règim jurídic d'aquest tipus de mesures provisionals en el si del procediment administratiu, i el seu encaix en l'ordre constitucional i la legislació bàsica del procediment administratiu.

A) Les mesures prèvies al procediment sancionador, també anomenades provisionalíssimes, són un tipus de mesures cautelars que poden ser adoptades amb caràcter previ a l'inici d'un procediment administratiu de naturalesa sancionadora. La seva finalitat té per objecte assegurar determinats drets, béns o interessos dignes de ser protegits per part de l'Administració pública davant d'un risc d'afectació per dany o pèrdua, abans que se substanciï i finalitzi un procediment administratiu mitjançant la corresponent resolució de l'òrgan competent.

Cal recordar que les mesures cautelars, amb caràcter general, i pel fet que anticipen una decisió prèvia, encara que sigui de manera parcial i provisional, al tancament, o fins i tot a l'inici, d'un procediment, suposen una excepció al règim general del procediment i de l'actuació administrativa, atès que el seu contingut pot col·lidir amb el dret a la presumpció d'innocència, modulat en l'àmbit sancionador administratiu, i protegit per la Constitució a través del dret fonamental de l'article 24 CE.

Així, una mesura cautelar que suposi una pèrdua o un menyscapte, ni que sigui transitori, de drets individuals, pot significar en realitat una sanció encoberta, la qual no té empara en un estat democràtic, entre altres raons, perquè podria conculcar, com s'ha dit, el principi d'innocència (STC 22/1985, de 15 de febrer, FJ 6). Ara bé, la seva adopció s'admet, en un procediment sancionador, sempre que es faci mitjançant una resolució fonamentada en

dret que, quan no és reglada, es basi en un judici de raonabilitat sobre la finalitat cercada i les circumstàncies concurrents, ja que una mesura desproporcionada o desraonada no seria cautelar sinó que tindria un caràcter punitiu quant a l'excés (STC 108/1984, de 26 de novembre, FJ 2.*b*).

Igualment, l'ús de les mesures provisionals prèvies al començament del procediment administratiu ha de ser extremadament acotat i restringit pel fet que tenen lloc abans de l'inici de les actuacions administratives i poden incidir en un dret, un bé o un interès d'un tercer sense que s'hagin practicat les proves que preveu el procés ni l'administrat hagi comptat amb els tràmits i les garanties que l'ordenament jurídic li reconeix. I això, en gran mesura, com hem dit, perquè poden produir una situació d'anticipació provisional de la decisió final amb un contingut que pot ser sancionador.

Aquesta configuració, en conseqüència, és susceptible d'afectar els drets del ciutadà concernit i d'interferir en el principi constitucional d'actuació objectiva de l'Administració, establert als articles 9.3 i 103 CE. No hem d'oblidar, com ha recordat insistentment la jurisprudència del Tribunal Constitucional, que l'objectivitat al servei dels interessos generals se situa als antípodes de l'arbitrarietat i la manca de la garantia dels drets dels administrats, els quals són assegurats pel compliment estricte dels diversos procediments i condicions que vinculen els poders públics mitjançant la subjecció a les lleis (per totes, STC 34/1995, de 6 de febrer, FJ 3).

Pel que fa a la legislació que les regula, aquesta tipologia de mesures cautelars està prevista actualment i expressa a l'article 56.2 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (LPACAP), si bé té el seu antecedent en l'article 72.2 de la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú (LRJAPC), com a conseqüència de la modificació operada per la Llei 4/1999, de 13 de

gener, que va introduir la possibilitat d'adoptar aitals mesures abans de l'inici del procediment administratiu.

A tall de síntesi, i pel que ara interessa, l'article 56.2 LPACAP admet la legitimitat de les mesures cautelars abans d'iniciar el procediment administratiu, sempre que se sotmetin als requisits següents: que es tracti d'una situació d'urgència inajornable, que la seva finalitat sigui la protecció provisional dels interessos implicats, que s'adoptin de forma motivada i que resultin necessàries i proporcionades. Addicionalment, exigeix que es confirmin, s'aixequin o es modifiquin en l'acord d'inici del procediment, el qual s'ha de dictar en un termini breu de quinze dies i pot ser objecte del corresponent recurs. I, finalment, afirma que les mesures restin sense efecte en cas de no iniciar-se el procediment en el termini esmentat o quan l'acord d'iniciació no contingui un pronunciament exprés sobre aquelles. Ultra això, també resultaria aplicable la previsió general que no es poden adoptar les que puguin causar un perjudici de difícil o impossible reparació als interessats o que impliquin violació dels drets emparats per les lleis (art. 56.4 LPACAP).

Val a dir que l'actual normativa de les mesures provisionals en el procediment administratiu comú, incloent-hi les de caràcter previ a l'inici d'aquest (art. 56 LPACAP), resulta també aplicable al procediment sancionador, que ha passat a considerar-se com un procediment administratiu comú, que se sotmet a les mateixes regles generals que aquest, sens perjudici d'algunes especialitats en la seva tramitació, que recull l'articulat de la mateixa Llei (art. 1 LPACAP). Certament, això constitueix una diferència significativa amb la regulació anterior (art. 72 LRJAPC), que no es projectava sobre els procediments administratius sancionadors, en els quals només es podien adoptar mesures provisionals si així ho preveien les normes sectorials que les regulessin «per mitjà d'un acord motivat» i per assegurar «l'eficàcia de la resolució final que es pugui dictar» (art. 136 LRJAPC).

Completava aquesta regulació el també ja derogat Reglament de procediment per a l'exercici de la potestat sancionadora (art. 15), aprovat pel Reial decret 1398/1993, de 4 d'agost.

Ara bé, tot i l'anterior, l'àmbit d'aplicació objectiu de la vigent LPACAP es redueix per allò que prescriu la seva disposició addicional primera sobre les especialitats per raó de la matèria, quan preveu que «[e]ls procediments administratius regulats en lleis especials per raó de la matèria que no exigeixin algun dels tràmits que preveu aquesta Llei o regulin tràmits addicionals o diferents es regeixen, respecte a aquests, pel que disposen les lleis especials esmentades» (apt. 1). D'altra banda, a continuació, la mateixa disposició estableix una llista de les actuacions i els procediments que es regeixen per la seva normativa específica i, supletòriament, pel que diu la LPACAP, entre els quals (aplicació dels tributs en matèria tributària i duanera, així com la seva revisió en via administrativa; gestió, inspecció, liquidació, recaptació, impugnació i revisió en matèria de Seguretat Social i desocupació; sancions en matèria tributària i duanera, en l'ordre social, en matèria de trànsit i seguretat viària i en matèria d'estrangeria, i estrangeria i asil) no es troba el procediment sancionador en matèria de xarxes i comunicacions electròniques (apt. 2).

En conseqüència, doncs, i com a regla general, s'ha d'interpretar que, quan una llei sectorial regula el tràmit procedimental per a l'adopció de mesures provisionals en un procediment sancionador (incloses les adoptades prèviament a l'inici d'aquest) de manera diferent a com ho fa l'article 56 LPACAP, preval l'aplicació d'aquesta especialitat per raó de la matèria, de manera que es plantejarien seriosos dubtes sobre si s'haurien d'observar o no en tot cas les garanties que en relació amb aquesta actuació cautelar preveu la LPACAP, a les quals acabem de fer referència.

B) A continuació, ens correspon examinar el contingut del precepte que ha estat objecte d'una nova redacció per part del Reial decret llei sotmès al nostre escrutini.

Abans, però, resulta d'utilitat fer referència als canvis principals que ha experimentat el seu contingut respecte de la versió de la LGTEL vigent fins al moment de l'aprovació del Reial decret llei 14/2019. Així, s'ha d'indicar que la potestat d'adoptar la mesura provisional de cessament de l'activitat infractora amb caràcter previ a l'inici del procediment sancionador que s'atribueix a l'Administració estatal ja estava prevista en la redacció original de la LGTEL de 2014, i que allò que ha variat és la configuració dels supòsits habilitants. En efecte, d'una banda, es mantenen els previstos anteriorment, però s'amplia el seu abast, com és el cas de la lletra *a*, que ara incorpora els conceptes «d'ordre públic» i de «seguretat nacional» o el de la lletra *b*, que ha substituït el concepte de «vida humana» pel més ampli de «salut pública». I, de l'altra, s'introdueix el supòsit de la lletra *e*, que habilita el cessament de la presumpta activitat infractora quan ocasioni greus problemes econòmics o operatius a un ampli ventall de destinataris del sector (a proveïdors o usuaris de xarxes o serveis de comunicacions electròniques i, en general, a tots els usuaris de l'espectre radioelèctric).

Per la seva part, a efectes interpretatius del conjunt de la norma, resulta il·lustratiu referir-nos a l'apartat 2 de l'article 81 LGTEL, tot i que no és objecte de la sol·licitud per no haver estat reformat, el qual disposa que la resolució que determini l'ordre de cessament de l'activitat afectada pot preveure el suport dels cossos i forces de seguretat per a l'execució forçosa, a través de l'autoritat governativa. Addicionalment, disposa que l'esmentada resolució determini l'àmbit objectiu i temporal de la mesura, que no pot excedir d'un mes.

La raó de la modificació de l'apartat 1 de l'article 81 LGTEL no consta clarament al preàmbul del Reial decret llei, que, en una al·lusió genèrica, es limita a dir que «en correlació necessària amb aquest reforçament de funcions públiques en aquestes situacions excepcionals, es potencia igualment la potestat sancionadora del Ministeri d'Economia i Empresa amb l'objectiu de fer efectives i reals les actuacions que pugui adoptar en ús d'aquestes noves facultats d'actuació dirigides a preservar o restablir l'ordre públic, la seguretat pública i la seguretat nacional» (apt. II, par. vint-i-vuitè).

Com acabem d'indicar, el nou redactat de l'article 81.1 LGTEL incorpora, en la línia del que ja hem analitzat en aquest mateix fonament jurídic amb motiu de l'article 4.6 LGTEL, nous supòsits habilitants per a l'adopció de mesures prèvies vinculats als conceptes d'ordre públic i seguretat nacional; salut pública, o en casos de «greus problemes econòmics o operatius a d'altres proveïdors o usuaris de xarxes de comunicacions i de l'espectre radioelèctric».

Resulta clar, doncs, que el marge de supòsits en els quals l'Administració pot apreciar la necessitat d'aplicar el cessament previ de l'activitat abans de començar el procediment sancionador s'ha incrementat respecte de la versió anterior del precepte, fins i tot en el cas de la seguretat pública, que passa d'una possible «activitat infractora» que pugui produir «perjudicis greus al funcionament dels serveis de seguretat pública, protecció civil i d'emergències» al més extens de «quan existeixi una amenaça immediata i greu per a l'ordre públic, la seguretat pública o la seguretat nacional». Així, aquest darrer supòsit s'amplia substancialment, en el sentit d'evolucionar d'una afectació més precisa i acotada a determinats serveis públics a un risc més genèric, més imprecís o més difós, malgrat la utilització, amb semblança restrictiva, de l'expressió d'amenaça «immediata i greu».

Per tant, de manera objectiva, el règim de les situacions que justifiquen l'adopció de mesures prèvies de l'article 81.1 LGTEL, més enllà de la comparativa amb la seva redacció de l'any 2014, és en si mateix remarcablement ampli, amb la inserció d'evidents conceptes jurídics indeterminats, els quals, i això és també rellevant, es desvinculen del règim de l'esquema normatiu sancionador de la matèria de telecomunicacions per situar-se en el de les presumptes amenaces sistèmiques: ordre públic, seguretat pública, salut pública, etc.

Aquesta caracterització de la norma, en la nostra tasca d'examinar-la, pren especial rellevància quan es connecta amb l'absència de previsió en el seu text de determinades garanties que són puntals en el règim jurídic de protecció en l'àmbit del dret administratiu dels drets fonamentals previstos a la Constitució. Ens estem referint, com hem indicat més amunt i també abans en aquest fonament jurídic, al fet que l'article 81.1 LGTEL no recull expressament en la seva lletra l'exigència que l'adopció de mesures prèvies requereix necessàriament la motivació de la resolució que les acorda o el mateix tràmit d'audiència de l'interessat.

És cert que el darrer paràgraf de l'apartat 2 de l'article 81 LGTEL (que no s'ha modificat pel Reial decret llei) diu que en la resolució «cal determinar l'àmbit objectiu i temporal de la mesura, sense que pugui excedir el termini d'un mes». Però, aquest incís és insuficient per complir, com veurem, les exigències respecte del contingut de la llei per habilitar una restricció legítima dels drets i les llibertats dels ciutadans per part de l'Administració pública. No consta en la norma la regla general que la mesura provisional de cessament hagi d'ésser necessària i proporcionada; tampoc que caldria confirmar-la, aixecar-la o modificar-la en l'acord d'inici del procediment si té lloc abans del termini establert d'un mes. Igualment, no es fa referència al possible recurs de la resolució que s'adopti i no es recull la circumstància que la mesura hauria de restar sense efecte en cas de no iniciar-se el

procediment en el termini esmentat o quan l'acord d'iniciació no contingui un pronunciament exprés sobre ella. Finalment, es troba a faltar la cautela general que no es poden acordar quan puguin causar un perjudici de difícil o impossible reparació als interessats o impliquin una violació dels drets dels administrats.

Ultra això, cal fer una darrera consideració crítica sobre l'exclusió expressa que fa l'article 81.1 LGTEL de l'audiència en la tramitació de la mesura provisional prèvia a l'inici del procediment. Respecte d'aquesta qüestió, és evident que l'audiència de l'afectat per la mesura és una garantia per a l'administrat que hauria de preservar-se sempre que així fos possible i com a regla general, per tal d'evitar la vulneració dels drets dels interessats o que es puguin ocasionar perjudicis de difícil o impossible reparació. El fet que el precepte la descarti de manera sistemàtica i apriorística, presumiblement per les mateixes raons d'imperiosa urgència a què fa referència, no ha d'impedir que aquest tràmit es realitzi el més aviat possible després d'adoptada la mesura de suspensió i abans de l'inici del procediment sancionador, a fi de valorar i, si escau, pal·liar els perjudicis que pot produir al destinatari de la mesura. Si s'inicia el procediment, resulta clar que s'han d'aplicar les regles comunes de la participació dels interessats, inclosa la corresponent al tràmit de l'audiència (art. 82 LPACAP).

Com hem reiterat, les mesures prèvies han de ser excepcionals i limitades a casos en els quals sigui estrictament necessària la seva adopció per protegir un interès, un dret o un bé d'interès públic que mereix ser salvaguardat i que, altrament, correria el risc de ser danyat o desaparèixer, i ha de consistir en una intervenció eficaç i, alhora, el menys constrictiva possible en relació amb els drets i les llibertats de la persona afectada, la qual ha de poder tenir la capacitat de defensar-se mitjançant el subsegüent sistema de recursos administratius i judicials.

Doncs bé, si retornem a l'article 81.1 LGTEL, comprovem que tant pel que fa als supòsits de justificació de la necessitat, a la manca de previsió explícita de garanties cabdals, com ara la motivació o l'exclusió expressa de l'audiència, obtenim la convicció que la regulació de l'article 81.1 LGTEL pateix de greus defectes quant a la seva qualitat legislativa, de manera que es tracta d'una norma que, pel seu objecte d'aplicació, és susceptible de restringir il·legítimament drets i llibertats emparats constitucionalment. Si a aquesta situació hi afegim que la LGTEL és una norma amb rang de llei, sectorial i que no figura entre la legislació a la qual s'aplica amb caràcter supletori l'article 56 LPACAP, podem arribar a la conclusió, o com a mínim se'ns generen seriosos dubtes, del tot raonables, que el precepte que estem examinant exonera de motivació la resolució mitjançant la qual s'adoptin les mesures prèvies al procediment sancionador, així com d'altres garanties que hem vist que haurien d'acompanyar aquest tipus de mesures cautelars.

Sobre l'objectivitat en les actuacions administratives (art. 9.3 i 103 CE), el dret a la presumpció d'innocència i el dret a la tutela judicial efectiva (art. 24 CE), hem de recordar que la jurisprudència constitucional sovint ha valorat el requisit essencial de la motivació com a condició necessària per escrutar l'objectiu i la proporcionalitat d'una mesura dictada pels poders públics i, així, poder descartar, o apreciar, si escau, l'arbitrarietat en l'exercici de la potestat pública sotmesa a l'imperi de la llei.

De fet, la doctrina constitucional ha declarat que les garanties processals establertes a l'article 24 CE són aplicables també als procediments administratius sancionadors, si tenim en compte que són manifestació de la potestat punitiva de l'Estat, amb les matisacions que resultin de la seva naturalesa mateixa (STC 17/2009, de 26 de gener, FJ 2). I, en el sentit exposat, ha ressaltat que una d'aquestes garanties és el deure de motivació que, quan es tracta dels actes de l'Administració en l'exercici de les seves potestats sancionadores, adquireix una dimensió constitucional, en la mesura

que limiten o restringeixen l'exercici de drets fonamentals (STC 82/2009, de 23 de març, FJ 2). D'acord amb l'anterior, destaca que una motivació satisfà les exigències de la tutela judicial sempre que exterioritzi els elements de judici sobre els quals es basa la decisió i quan de la seva fonamentació resulti una aplicació no irracional, no arbitrària o no manifestament errònia de la legalitat (STC 21/2008, de 31 de gener, FJ 3). Així mateix, ha declarat que l'exigència que una resolució estigui motivada permet el seu control posterior i, d'aquesta manera, s'evita tota arbitrarietat (STC 140/2009, de 15 de juny, FJ 3).

Precisament, és la motivació de la resolució l'element que aporta la fonamentació de la justificació de la necessitat, és a dir la connexió raonable entre causa (risc) i efecte (potencial dany), i la proporcionalitat de la mesura prèvia, consistent en la ponderació entre l'eficàcia o idoneïtat de l'acció acordada i el cost de protegir el dret o l'interès que es pretén assegurar. Sense l'explicitació d'aquests arguments, suport cognitiu del dret com a expressió de la raó, difícilment es pot distingir entre discrecionalitat i arbitrarietat, i més difícil encara és garantir l'aparell de drets i llibertats dels ciutadans sotmesos al poder de policia de l'Administració.

Tanmateix, i partint de la validesa dels arguments que acabem d'exposar, som conscients que alternativament també es podria realitzar, tot i que entenem que de manera forçada, una interpretació en el sentit que l'article 56 LPACAP podria ser d'aplicació supletòria a l'article 81.1 LGTEL, atès el silenci que manifesta el precepte en qüestió, però el cert és que, com hem indicat, les condicions que evidencia la seva regulació ens mantenen ferms en la nostra conclusió negativa. Així, el fet que una norma amb rang de llei, reformada amb posterioritat a la LPACAP, i de caràcter més sectorial, com és la LGTEL, prevegi un procediment sancionador específic que inclou un tràmit singular de mesures provisionals prèvies a l'inici de les actuacions administratives sancionadores, que guarda silenci sobre garanties tan

cabdals com la motivació i que exclou expressament el tràmit d'audiència prèvia i no fa esment de la seva posterior substanciació, al mateix temps que preveu un termini propi per al seu aixecament diferent i més llarg que l'establert a la normativa administrativa general (1 mes en lloc de 15 dies), i que pot ser aplicat per constrènyer drets constitucionals, ens condueix a apreciar, de manera natural i raonable, l'evident insuficiència, per no dir deficiència, de la seva qualitat normativa, que, en termes de tècnica legislativa clara i previsible, és de difícil adequació constitucional. Defensar una interpretació de constitucionalitat, en tot cas, ens sembla un exercici tan esforçat com voluntarista, que no hauria de tenir cabuda ni pot ser vàlid quan es tracta de preceptes que limiten els drets i interessos dels ciutadans, sobretot per part de les autoritats governatives o administratives, i al marge d'un procediment amb totes les garanties degudes. I això encara més tractant-se d'una mesura de cessament de l'activitat, que anticipa un cert caràcter sancionador i que pot comportar greus perjudicis per als interessos dels afectats.

En conclusió, l'apartat cinc de l'article 6 RDL 14/2019, de 31 d'octubre, en la modificació que efectua de l'apartat 1 de l'article 81 de la Llei 9/2014, de 9 de maig, general de telecomunicacions, és inconstitucional perquè pateix d'uns defectes de qualitat normativa, quant a les condicions d'exercici de la potestat de dictar mesures prèvies al procediment sancionador en matèria de telecomunicacions, tant pel que fa a la incorporació de les garanties dels ciutadans com a la previsibilitat de la seva aplicació, que el fan incompatible amb el principi de seguretat jurídica *ex* article 9.3 CE, així com amb les exigències de la jurisprudència del Tribunal Constitucional i el Tribunal Europeu de Drets Humans per a les lleis que limiten drets fonamentals, en aquest cas el dret a la presumpció d'innocència i a la tutela judicial efectiva aplicats a l'àmbit del dret administratiu sancionador (art. 24 CE).

4. L'article 6.dos RDL introdueix un nou apartat 3 a l'article 6 LGTEL, en els següents termes:

> «3. Les administracions públiques han de comunicar al Ministeri d'Economia i Empresa qualsevol projecte d'instal·lació o explotació de xarxes de comunicacions electròniques en règim d'autoprestació que faci ús del domini públic, tant si aquesta instal·lació o explotació s'ha d'efectuar de manera directa, a través de qualsevol entitat o societat dependent d'aquella, o a través de qualsevol entitat o societat a la qual se li hagi atorgat una concessió o habilitació a l'efecte.
> El règim d'autoprestació en la instal·lació o explotació de la xarxa esmentada pot ser total o parcial, i per tant la comunicació s'ha d'efectuar encara que la capacitat excedent de la xarxa es pugui utilitzar per a l'explotació per part de tercers o per a la prestació de serveis de comunicacions electròniques disponibles al públic.
> En cas que s'utilitzi o que estigui previst utilitzar, directament per part de l'Administració pública o per part de tercers, la capacitat excedent d'aquestes xarxes de comunicacions electròniques en règim d'autoprestació, el Ministeri d'Economia i Empresa ha de verificar el compliment del que preveu l'article 9. A aquest efecte, l'Administració pública ha de proporcionar al Ministeri d'Economia i Empresa tota la informació que li requereixi a l'efecte de verificar-ne el compliment.
> L'obligació que estableix aquest apartat s'entén sense perjudici de la que preveu l'article 7.3 d'aquesta Llei.»

A) L'anàlisi del precepte citat requereix que, en primer lloc, realitzem una referència prèvia al règim d'actuació de l'Administració pública en l'àmbit de les telecomunicacions.

La LGTEL, com hem vist, preveu dos tipus d'intervencions de les administracions públiques en l'àmbit de les comunicacions electròniques: d'una banda, les actuacions d'explotació de xarxes i/o prestació de serveis de

comunicacions electròniques a tercers i, d'una altra, les actuacions en règim d'autoprestació.

En el primer supòsit, les administracions públiques únicament poden actuar com a operadors a través d'entitats o societats controlades directament o indirecta, l'objecte social de les quals inclogui la instal·lació i l'explotació de xarxes o la prestació de serveis de comunicacions electròniques (art. 9.2 i 9.3 LGTEL). Aquesta activitat de l'Administració queda subjecta al règim de la LGTEL, per tal de garantir la prestació dels serveis sota condicions de mercat i criteris d'inversor privat, d'acord amb els principis de separació de comptes, neutralitat, transparència, no-distorsió de la competència i no-discriminació, i en compliment de la normativa sobre ajuts d'Estat, evitant d'aquesta manera que es produeixin pertorbacions de la competència (apt. III, par. cinquè preàmbul i art. 9 LGTEL). Abans de l'inici de l'activitat, es preveu l'obligació de comunicació al Registre d'operadors, el qual depèn del Ministeri d'Indústria, Energia i Turisme (tot i que la seva gestió correspon transitòriament a la Comissió Nacional dels Mercats i la Competència —en endavant, CNMC— d'acord amb la disposició transitòria desena LGTEL), on s'inscriuran les dades relatives a l'operador controlat directament o indirecta per l'Administració amb caràcter declaratiu (art. 6.2 i 7 LGTEL i art. 5.4, 5.5, 7 i següents del Reial decret 424/2005, de 15 d'abril, pel qual s'aprova el Reglament sobre les condicions per a la prestació de serveis de comunicacions electròniques, el servei universal i la protecció dels usuaris). Un cop realitzada la notificació, l'interessat adquireix la condició d'operador i pot començar la prestació del servei o l'explotació de la xarxa (art. 5.1 Reial decret 424/2005).

En el cas d'autoprestació, que és la que és objecte de la present anàlisi, l'Administració pública pot desenvolupar la seva activitat al marge del règim general de lliure competència que és inherent a l'explotació de xarxes i la prestació de serveis de comunicacions electròniques (art. 5 LGTEL). Això no

obstant, està obligada a notificar al Registre d'operadors el projecte d'instal·lació o explotació de les xarxes de comunicacions electròniques que facin ús del domini públic, tant si aquesta instal·lació o explotació es realitza de manera directa com a través de qualsevol entitat o societat (art. 7.3 LGTEL). L'esmentada comunicació únicament s'ha de referir als projectes i no és objecte d'inscripció en el Registre d'operadors en la mesura que, com veurem tot seguit, no es tracta d'una explotació de xarxes disponibles per al públic en general (art. 6 LGTEL; art. 5.4 Reial decret 424/2005).

Quant al significat del terme «autoprestació», la Comissió del Mercat de les Telecomunicacions (actualment integrada en la CNMC) ha precisat que s'entén com a tal l'explotació de xarxes i la prestació de serveis de comunicacions electròniques per una administració pública «para la satisfacción de sus necesidades, esto es, las vinculadas al desempeño de las funciones propias del personal al servicio de la Administración Pública de que se trate y que contribuyan al cumplimiento de los fines que le son propios» (art. 3.1 Circular 1/2010, de 15 de juny de 2010, per la qual s'estableixen les condicions per a l'explotació de xarxes i la prestació de serveis de comunicacions electròniques per les administracions públiques). En aquest supòsit s'inclouen els centres d'educació o formació d'ensenyament reglat, com ara escoles, instituts, col·legis i centres universitaris així com l'àrea dels seus campus, entenent que tant alumnes com professors formen part del personal indispensable per al desenvolupament de les tasques del centre (art. 3.2 Circular 1/2010). S'assimilen a l'autoprestació, entre d'altres, el servei d'accés a internet limitat a les pàgines web de les administracions que tinguin competències en l'àmbit territorial en què es presti aquest servei, el servei general d'accés a internet en biblioteques (annex Circular 1/2010) i les activitats que no es consideren dirigides al públic en general, com ara l'accés a internet a museus, mercats o hospitals públics (Acord CNMC de 13 de febrer de 2019, CNS/DTSA/131/19, amb citació de diversos acords de la Sala de Supervisió Regulatòria de l'organisme).

Dit això, cal puntualitzar que en els supòsits en els quals la xarxa tingui capacitat excedentària i s'utilitzi la mateixa infraestructura per prestar serveis majoristes o minoristes a tercers, l'Administració pública té la consideració, quant a aquests, d'explotadora de xarxes o prestadora de serveis de comunicacions electròniques a tercers i, per tant, resta subjecta al règim per a l'explotació de xarxes i la prestació de serveis de comunicacions electròniques per les administracions públiques que preveu la Circular 1/2010 (art. 3.3).

L'article 6.3 LGTEL, segons redacció donada pel Reial decret llei objecte de dictamen, incorpora a aquest règim d'autoprestació un nou deure de comunicar al Ministeri d'Economia i Empresa el projecte d'instal·lació o explotació de xarxes en règim d'autoprestació que facin ús del domini públic, tant si l'activitat es realitza de manera directa com indirecta, que s'afegeix a l'obligació de notificació al Registre d'operadors que ja hem vist que preveu l'article 7.3 LGTEL (primer par.). Així mateix, disposa que en cas que l'esmentada xarxa de comunicacions electròniques en règim d'autoprestació tingui capacitat excedentària i s'utilitzi o estigui previst fer-ne ús, directament per l'Administració pública o per tercers, el Ministeri haurà de verificar el compliment de les exigències de l'article 9 LGTEL. Això és, si es respecten o no les normes aplicables a l'explotació de xarxes i la prestació de serveis de comunicacions electròniques en règim de prestació a tercers per part de les administracions públiques i, per tant, a través d'operadors controlats per aquestes. De forma complementària, s'afegeix que l'Administració pública afectada «ha de proporcionar al Ministeri d'Economia i Empresa tota la informació que li requereixi a l'efecte de verificar-ne el compliment» (tercer par.).

Addicionalment, les administracions públiques han de comunicar al Ministeri d'Economia i Empresa, en el termini d'un mes des de l'entrada en vigor del

Reial decret llei, les xarxes de comunicacions electròniques en règim d'autoprestació que utilitzin el domini públic a les quals es refereix l'article 6.3 LGTEL, i que hagin estat instal·lades o estiguin en procés d'instal·lació o explotació (disp. add. única RDL).

B) El peticionari qüestiona des d'una perspectiva competencial el nou article 6.3 LGTEL i, més concretament, la facultat «d'intervenció i control preventiu» mitjançant la «tècnica de la comunicació» que reconeix a l'Administració general de l'Estat, entenent que podria constituir una extralimitació de la competència estatal de l'article 149.1.21 CE i una invasió de la competència de la Generalitat reconeguda a l'article 140.7 EAC, particularment quant a la competència executiva sobre la promoció de l'existència d'un conjunt mínim de serveis d'accés universal.

Per tal de donar resposta a la sol·licitud, i fetes les consideracions anteriors, hem d'enquadrar competencialment els preceptes dictaminats i determinar si l'Estat està legitimat d'acord amb el bloc de la constitucionalitat per a la seva adopció.

La disposició final primera RDL 14/2019 identifica com a títol competencial habilitant de l'article 6 la competència estatal de l'article 149.1.21 CE en matèria de règim general de comunicacions.

En vista del seu contingut i la seva finalitat, l'article 6.3 LGTEL i la disposició addicional única RDL 14/2019 incideixen efectivament en el règim d'explotació de les xarxes i de prestació dels serveis de comunicacions electròniques, el qual s'insereix dins la matèria del règim general de comunicacions (STC 8/2012, FJ 7), sobre la qual, com hem vist, correspon a l'Estat *ex* article 149.1.21 CE la totalitat de la competència normativa i fins i tot la funció executiva necessària per configurar un sistema materialment unitari.

Aquest títol comprèn, pel que ara interessa, la regulació de la competència en el mercat i les obligacions de fer i de no fer dels operadors del sector (STC 8/2016, de 21 de gener, FJ 2). I, per tant, en paraules del Tribunal Constitucional, l'Estat, en exercici de la seva competència de l'article 149.1.21 CE, «ha decidido caracterizar [el sector] como un sector abierto a la libre competencia cuyas particulares características, sin embargo, determinan no solo una regulación más intensa por parte de los poderes públicos, sino también la posibilidad de establecer excepciones a aquel principio cuando sea necesario para alcanzar determinados objetivos […]. Y es también la Administración del Estado la que define los servicios cuya prestación por los poderes públicos no supone una distorsión de la libre competencia del sector, bien por tratarse de una autoprestación bien porque, aun prestándose de forma gratuita e ininterrumpida por el poder público, se entiende que no alteran la estructura del mercado» (STC 8/2016, FJ 6).

Un cop determinada la inserció de l'article 6.dos RDL 14/2019 en la matèria del règim general de les comunicacions, cal escatir si aquesta competència admet l'establiment d'un deure de comunicació a l'Administració de l'Estat dels projectes relatius a xarxes de comunicacions electròniques en règim d'autoprestació que facin ús del domini públic. Una comunicació que, en darrera instància, li permet verificar el compliment dels requisits per a l'ús de la capacitat excedentària d'aquestes xarxes, els quals tenen com a finalitat salvaguardar els principis d'inversor privat, neutralitat, transparència, no-distorsió de la competència i no-discriminació propis d'un mercat liberalitzat com és el de les telecomunicacions, però amb forta intervenció pública, com hem dit al principi d'aquest fonament jurídic (art. 107 i 108 TFUE i art. 9 LGTEL).

Als efectes del present Dictamen, cal recordar que la LGTEL, a més de la comunicació al Registre de l'article 7.3, ja preveu mecanismes de

subministrament d'informació a l'Estat per part de les persones físiques o jurídiques que exploten xarxes o presten serveis de comunicacions electròniques i agents que intervenen en el mercat a petició de les autoritats nacionals de reglamentació de telecomunicacions (art. 10), és a dir, el Govern, els òrgans superiors i directius del Ministeri d'Indústria, Energia i Turisme i del Ministeri d'Economia i Competitivitat competents i la CNMC (art. 68). La Llei dedica també el seu títol VIII a la regulació de les potestats d'inspecció i sanció en la matèria.

Malgrat aquest marc (art. 7.3 i 10 LGTEL), el Reial decret llei 14/2019 imposa ara noves obligacions a les administracions públiques: la comunicació al Ministeri del projecte d'instal·lació o d'explotació de xarxes en règim d'autoprestació tant si «s'ha d'efectuar de manera directa» o indirecta i l'obligació de subministrament d'informació «[e]n cas que s'utilitzi o que estigui previst utilitzar» la capacitat excedentària de les dites xarxes, en el darrer cas, a l'efecte que l'Administració estatal verifiqui el compliment dels requisits previstos a l'article 9 LGTEL.

Ara bé, aquest règim de control específic no està suficientment explicitat pel legislador estatal, atès que el precepte no concreta els aspectes procedimentals ni els efectes de la comunicació o de la verificació realitzada per l'Administració de l'Estat, essent per tant incertes quines serien les conseqüències de l'incompliment o el compliment defectuós per part de l'operador/Administració pública, a criteri d'aquella, dels requisits previstos a l'article 9 LGTEL.

En conseqüència, es planteja la pregunta cabdal consistent a determinar quin és el motiu d'aquesta doble comunicació i d'una facultat de verificació afegida que incorpora de bell nou el Reial decret llei 14/2019. I, si bé no es dedueix immediatament del text del precepte, la resposta sí que es pot arribar a desprendre del preàmbul de la norma.

Així, aquest justifica l'article 6 i les reformes que impulsa de la LGTEL «per afrontar situacions que poden afectar el manteniment de l'ordre de públic, la seguretat pública o la seguretat nacional». En concret, respecte dels articles 4.6 i 6.3 LGTEL, al·lega que els modifica per reforçar les potestats del Ministeri d'Economia i Empresa per realitzar un major control i millorar «les seves possibilitats d'actuació quan la comissió d'una presumpta actuació infractora a través de l'ús de les xarxes i els serveis de comunicacions electròniques pugui suposar una amenaça greu i immediata per a l'ordre públic, la seguretat pública o la seguretat nacional o quan en determinats supòsits excepcionals que també puguin comprometre l'ordre públic, la seguretat pública i la seguretat nacional sigui necessària l'assumpció de la gestió directa o la intervenció de les xarxes i els serveis de comunicacions electròniques» (apt. II, par. vint-i-cinquè preàmbul RDL 14/2019).

Aquesta afirmació, com a manifestació dels objectius cercats pel legislador estatal, ens connecta necessàriament amb l'article 4.6 LGTEL, que hem analitzat en aquest mateix fonament jurídic i evidencia, per tant, el seu caràcter instrumental: els mecanismes previstos en la nova versió de l'article 6.3 LGTEL, de comunicació doblada i de potestat de verificació estatal, tenen per finalitat contribuir a obtenir informació rellevant per a l'activació de la facultat d«'intervenció» governamental en les xarxes de comunicacions electròniques.

Respecte dels raonaments sobre la manca de qualitat normativa vinculada a aquesta capacitat genèrica i indeterminada d'ingerència administrativa, ens remeten al què ja hem exposat, i a efectes de la present anàlisi ens resulta suficient amb recordar que la facultat «d'intervenció» emparada en els supòsits habilitants de la seguretat pública i l'ordre públic, deslligada del règim de la contractació administrativa (a diferència de la versió de la LGTEL de 2014 que la situava en aquest marc legal) i sense preveure cap

autorització judicial, és incompatible amb les garanties normatives exigibles a tota llei que pugui afectar a drets i llibertats constitucionals.

Per tant, si l'article 6.3 LGTEL que estem examinant s'apliqués en el sentit d'utilitzar els mecanismes que preveu (el deure de comunicació i la funció de supervisió) de forma mediata o subordinada en relació amb l'article 4.6 LGTEL, entenem que actuaria de manera espúria respecte del seu contingut objectiu. I, consegüentment, aquesta pràctica no seria legítima ni ajustada al sentit literal de la seva configuració ni al context normatiu que conforma el conjunt de la LGTEL.

Sobre el supòsit de l'assumpció transitòria de la gestió directa per part de l'Estat, també en el mateix sentit que hem resolt l'article 4.6 LGTEL, no apreciem cap retret d'inconstitucionalitat, atès que permet una interpretació vinculada a la garantia de la prestació dels serveis de telecomunicacions, per la seva condició de servei d'interès general econòmic i servei universal, en situacions acotades per la norma; és a dir, situacions excepcionals en què resultin afectades la seguretat pública i la seguretat nacional. Per tant, amb caràcter ordinari, la Generalitat de Catalunya pot adoptar les mesures que consideri adequades per garantir la prestació dels serveis i les xarxes de comunicació electròniques que siguin de la seva competència (art. 140.7 EAC).

En conclusió, l'apartat tres de l'article 6 i la disposició addicional única RDL 14/2019, malgrat que pot interpretar-se que manifesten una connexió instrumental amb l'article 4.6 LGTEL, segons es desprèn del preàmbul, i que el seu contingut esdevé sobrer o innecessari tenint en compte les facultats d'obtenció d'informació i de control que la LGTEL, en els seus diversos àmbits, atribueix a l'Estat, per si sols i en els termes en què estan redactats no evidencien una tatxa d'inconstitucionalitat pel que fa a la distribució de

competències entre l'Estat i la Generalitat *ex* articles 149.1.21 CE i 140.7 EAC.

5. L'article 7 RDL 14/2019, introdueix un nou apartat 3 a l'article 11 del Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació, que diu:

> «3. El Centre Criptològic Nacional (CCN) exerceix la coordinació nacional de la resposta tècnica dels equips de resposta a incidents de seguretat informàtica (CSIRT) en matèria de seguretat de les xarxes i els sistemes d'informació del sector públic comprès a la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, i a la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
> Els CSIRT de les administracions públiques han de consultar, quan escaigui, els òrgans amb competències en matèria de seguretat nacional, seguretat pública, seguretat ciutadana i protecció de dades de caràcter personal i hi han de col·laborar en l'exercici de les seves funcions respectives.
> El CCN exerceix la funció d'enllaç per garantir la cooperació transfronterera dels CSIRT de les administracions públiques amb els CSIRT internacionals, en la resposta als incidents i la gestió de riscos de seguretat que els corresponguin.»

A) Abans de delimitar el paràmetre aplicable a la norma, cal precisar l'objecte i la finalitat de l'apartat 3 de l'article 11 del Reial decret 12/2018, com també el seu context i marc normatiu, configurat per normes europees, estatals i autonòmiques.

Respecte del marc europeu on s'insereix principalment l'article examinat, cal fer esment a la Directiva 2016/1148, de 6 de juliol de 2016, del Parlament Europeu i del Consell, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i els sistemes d'informació en la Unió (Directiva NIS, per les sigles *Network and Information Systems*), la qual,

davant de nivells de seguretat fragmentats dins de la Unió, té per objecte assolir aquest nivell mínim i igual per tots els estats membres. I l'anterior, d'una banda, perquè les xarxes i els sistemes d'informació, sobretot internet, contribueixen de manera decisiva al desenvolupament de les activitats socials i econòmiques i del mercat interior, i de l'altra, per la constatació de la magnitud, la freqüència i els efectes dels incidents de ciberseguretat que, amb independència del lloc on es produeixin, poden afectar diferents estats membres i la Unió en el seu conjunt, atès el caràcter transversal de les xarxes i els sistemes (considerants 2, 3 i 5 i art. 1).

A fi de donar una resposta efectiva als problemes de seguretat de les xarxes i els sistemes d'informació, la citada norma europea conté un plantejament global que integra requisits mínims comuns en matèria de desenvolupament de capacitats i planificació, intercanvi d'informació, cooperació i requisits comuns de seguretat aplicables als operadors de serveis essencials (que són els que identifiquen els estats membres, i estan vinculats amb infraestructures) i als operadors de serveis digitals (que són els que tenen caràcter transfronterer i per aquest motiu se sotmeten a un règim d'harmonització màxima) (considerant 6 i art. 5 i 16). Val a dir que la Directiva NIS només resulta aplicable a les administracions públiques quan hagin estat identificades com a operadors de serveis essencials. D'aquesta manera, pel que fa a la resta de les xarxes i els sistemes d'informació de les administracions públiques, declara que correspon als estats la responsabilitat de garantir la seva seguretat (considerant 45).

En definitiva, es tracta de preservar la seguretat de les xarxes i els sistemes d'informació evitant tota acció que comprometi la disponibilitat, autenticitat, integritat o confidencialitat de les dades emmagatzemades, transmeses o tractades, o dels serveis oferts per aquestes xarxes i sistemes d'informació o accessibles a través seu (art. 4.2). Entre les mesures de prevenció, detecció, resposta i mitigació dels incidents i possibles riscos, es destaca l'obligació de

designar en cada estat una o més autoritats públiques competents en matèria de seguretat de les xarxes i els sistemes (art. 8.1) i la creació d'una xarxa d'equips de resposta a incidents de ciberseguretat informàtica o CSIRT, que són els que reben les notificacions dels incidents de seguretat (considerant 32 i art. 9). Els estats membres s'han d'assegurar que disposen de CSIRT que funcionin adequadament i amb capacitat per fer front als incidents i riscos i han de vetllar per una cooperació eficaç a escala de la Unió. Addicionalment, han de garantir que tots els operadors es trobin coberts per un CSIRT designat (considerant 34 i art. 9.1). I, donat que la major part de les xarxes i els sistemes d'informació són de gestió privada, la Directiva considera de vital importància la cooperació d'aquest sector amb el sector públic i anima els primers a crear els propis mecanismes de cooperació informal (considerant 35).

Altrament, cada Estat membre ha de designar un punt de contacte únic en matèria de seguretat de les xarxes i els sistemes d'informació (art. 8.3). Aquest punt de contacte actuarà d'enllaç per garantir la cooperació transfronterera entre les autoritats dels estats membres, amb les autoritats competents en els altres estats membres i amb el grup de cooperació (format per representants d'estats membres, la Comissió i ENISA), encarregat de donar suport i facilitar la cooperació estratègica i intercanvi d'informació entre els estats membres i desenvolupar confiança i seguretat, i la xarxa de CSIRT nacionals (art. 8.4)

Aquesta xarxa de CSIRT nacionals, creada per la Directiva 2016/1148 amb funcions d'intercanvi d'informació, suport i assistència mútues, cooperació operativa i seu de debat i anàlisi, està formada per representants dels CSIRT dels estats membres, per la Comissió, que hi participa en qualitat d'observador, i per ENISA, que es fa càrrec de la secretaria, promovent activament la cooperació entre els CSIRT (art. 12).

Vist això, resulta clar que són pilars bàsics de la regulació europea en l'àmbit que ens ocupa els mecanismes de cooperació i col·laboració, tant a nivell estatal com europeu i internacional, i el sistema de notificació d'incidents. En concret, quan en un mateix estat siguin òrgans distints l'autoritat pública competent, el punt de contacte únic i els CSIRT, aquests hauran de cooperar entre ells respecte al compliment de les obligacions establertes a la Directiva, com també els dos primers hauran d'informar els darrers sobre les notificacions dels incidents de seguretat objecte de la dita regulació (art. 10.1 i .3).

Cal assenyalar que la xarxa de CSIRT, creada per aquesta Directiva 2016/1148, també exerceix funcions de suport, assistència, assessorament i col·laboració a les administracions públiques per combatre riscos i incidents de seguretat i vetllar per la integritat i disponibilitat de les xarxes de comunicacions electròniques públiques, tot i que, com hem vist, aquelles no estan incloses en el seu àmbit d'aplicació específic [així ho disposa la Directiva (UE) 2018/1972, del Codi europeu de comunicacions electròniques, en el seu considerant 98]. En un altre ordre de coses, sobre denúncies que poden contribuir a la revelació d'infraccions de la Directiva NIS, podem esmentar la Directiva (UE) 2019/1937 del Parlament Europeu i del Consell de 23 d'octubre de 2019.

En l'àmbit estatal, s'ha de fer esment al Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació, modificat ara per la norma objecte del Dictamen, que ha transposat el contingut de la Directiva 2016/1148, si bé amb un àmbit d'aplicació subjectiu més ampli amb vista a assolir un enfocament global (art. 2). Per garantir l'esmentada seguretat, el Reial decret llei 12/2018 estableix un sistema de notificació d'incidents i un marc institucional de coordinació entre autoritats competents i amb els òrgans de cooperació rellevants de l'àmbit comunitari (art. 1). En aquest sentit, designa quines són les autoritats competents (art. 9) i

desenvolupa a nivell estatal la xarxa CSIRT creada per la Directiva, definint aquests organismes com els equips de resposta a incidents que analitzen riscos i supervisen incidents a escala estatal, difonen alertes sobre aquests incidents i aporten solucions per mitigar els seus efectes (art. 11 i 12). Val a dir que el legislador declara optar pel terme CSIRT, que és el comunament utilitzat a Europa, en lloc del terme CERT (*Computer Emergency Response Team*), registrat als EUA.

Pel que fa al punt de contacte únic exigit per la Directiva NIS, atribueix aquesta funció al Consell de Seguretat Nacional (art. 13). Als efectes del present Dictamen, cal dir que el RDL 12/2018 declara que té la condició de CSIRT de referència en matèria de seguretat de les xarxes i els sistemes d'informació respecte de la comunitat constituïda per les entitats públiques incloses en la LRJSP el Centre Criptològic Nacional (CCN-CERT) (art. 11.1.*a*.1), que fou creat pel Reial decret 421/2004, de 12 de març, adscrit al Centre Nacional d'Intel·ligència (Llei 11/2002, de 6 de maig). Aquest organisme es configura com una línia de defensa enfront dels ciberatacs, assumint la responsabilitat en ciberatacs sobre sistemes classificats, així com de les administracions públiques i empreses i organitzacions d'interès estratègic. La seva missió és reduir els riscos i les amenaces provinents del ciberespai, potenciant les accions no únicament defensives sinó primordialment preventives, correctives i de contenció, oferint servei tant a les administracions públiques com a les empreses d'interès estratègic, com, per exemple, el «Servicio de Alerta Temprana», i el desenvolupament de diferents eines, com les APT (Advanced Persistent Threat) i la Llista de coordinació d'incidents i amenaces, el «Informe Nacional del Estado de Seguridad», el «Motor de análisis remoto de troyanos avanzado», les guies CCN-STIC o els centres de seguretat.

Els CSIRT i/o els CERT que, com hem vist, són el grup d'experts responsables del desenvolupament de les mesures preventives i reactives

davant incidents de seguretat en els sistemes d'informació, poden ser públics o privats. En el supòsit que una organització no tingui el seu propi equip de resposta pot informar d'incidents als CSIRT o CERT públics, cosa que ajuda a assegurar-ne el diagnòstic i preveure incidents futurs.

Altres normes relacionades amb el tema de la seguretat en les xarxes de comunicació i els sistemes d'informació són la Llei 8/2011, de 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques i l'Esquema Nacional de Ciberseguretat 2019, publicat per l'Ordre PCI/487/2019, de 26 d'abril, i aprovat pel Consell de Seguretat Nacional.

En l'àmbit autonòmic, hem de destacar la Llei 15/2017, de 25 de juliol, de l'Agència de Ciberseguretat de Catalunya, que atribueix a aquesta autoritat pública la missió de garantir la ciberseguretat, entesa com la seguretat de les xarxes de comunicacions electròniques i dels sistemes d'informació (art. 2.1). Així mateix, exerceix les funcions d'equip de resposta a emergències (CERT), incloent-hi la relació amb altres organismes de ciberseguretat estatals i internacionals, i la coordinació dels equips de resposta a incidents de ciberseguretat (CSIRT) i equips de resposta a emergències o entitats equivalents que actuïn en llur àmbit territorial. A més, ha d'exercir aquestes funcions com a equip de resposta a emergències del Govern (art. 2.4.*c*); ha de col·laborar amb els organismes judicials i policials d'acord amb el que estableix la normativa vigent, i, en especial, s'ha de coordinar amb els cossos policials per a la ciberseguretat i protecció dels sistemes d'informació, d'acord amb les competències que tenen reconegudes en la matèria (art. 2.6).

Val a dir que l'esmentada Llei 15/2017 ha estat objecte de pronunciament pel Tribunal Constitucional a la STC 142/2018, a la qual ja hem fet referència en el fonament jurídic tercer i tornarem a tractar més endavant. Es pot avançar, però, que l'esmentada Resolució ha avalat la seva creació i les

seves funcions amb caràcter general, si bé les ha circumscrit a l'àmbit de Catalunya, com a dirigides a protegir i millorar la seguretat de les xarxes i a alertar davant l'existència de ciberamenaces relacionades amb l'Administració de la Generalitat i els seus sistemes d'informació i comunicacions propis, com també els dels particulars i de les altres administracions públiques que es relacionin amb ella per mitjans electrònics (FJ 7).

En aquest sector, recentment, s'ha aprovat l'Estratègia de Ciberseguretat de la Generalitat de Catalunya per al període 2019-2022, que defineix l'estratègia a seguir per aquesta última al llarg d'aquest període en matèria de ciberseguretat i dins l'àmbit de les administracions públiques de Catalunya, el seu sector públic, la ciutadania i aquelles entitats que, en qüestions de relacions administratives i/o comercials, tracten la informació, actius o infraestructures TIC titularitat de la Generalitat de Catalunya. En aquest document es confirma l'Agència de Ciberseguretat de Catalunya (en endavant ACC) com el principal organisme públic competent en aquest àmbit d'actuació.

A l'últim, més enllà de la normativa europea, estatal i autonòmica, cal fer èmfasi en el fet que el bé a protegir és la pròpia resposta als incidents de seguretat informàtica de tal manera que actors públics i privats relacionats amb la ciberseguretat es trobin en el que hom ha anomenat *Information Sharing*, concepte centrat en el procediment que permet recopilar, emmagatzemar i distribuir la informació necessària per actuar de forma homogènia, ràpida i eficaç contra les ciberamenaces.

B) Un cop descrit a grans trets el panorama normatiu actual, dilucidarem la distribució constitucional i estatutària de competències aplicable a la matèria objecte d'examen, tenint en compte que, com és sabut, la transposició a

l'ordenament intern del dret europeu ha de respectar en tot cas aquesta distribució competencial.

La disposició final primera del Reial decret llei declara que el seu article 7 ha estat dictat a l'empara de les competències estatals sobre règim general de les telecomunicacions i seguretat pública, previstes a l'article 149.1 CE, apartats 21 i 29, respectivament.

El sol·licitant, fent citació de la doctrina constitucional (STC 142/2018, de 20 de desembre), recorda que la Generalitat és competent, «com a administració electrònica i en compliment de la legislació estatal, per a l'adopció de les mesures adreçades a protegir les xarxes, sistemes d'informació i les infraestructures tecnològiques de l'Administració de la Generalitat i el seu sector públic i dels particulars i altres administracions públiques que s'hi relacionin per mitjans electrònics». I, en concret, diu que «[l]es noves previsions de coordinació de l'article 7 RDL 14/2019, a més d'incidir en els àmbits competencials de la Generalitat desplaçant la seva competència en la matèria, també podrien considerar-se desproporcionades, atès allò previst a la Directiva (UE) 2016/1148, del Parlament Europeu i del Consell, de 6 de juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i sistemes d'informació a la Unió, on un dels objectius reconeguts és la contribució i el desenvolupament de la confiança i seguretat entre Estats».

La norma objecte de dictamen, transcrita a l'inici d'aquest apartat, atribueix al Centre Criptològic Nacional (CCN) la coordinació estatal de totes les autoritats o equips de resposta a incidents de seguretat informàtica (CSIRT) en matèria de seguretat de les xarxes i els sistemes d'informació. Addicionalment, obliga tots els CSIRT de les administracions públiques a col·laborar en l'exercici de les funcions respectives i a consultar, quan escaigui, als òrgans amb competències en matèria de seguretat nacional,

seguretat pública, seguretat ciutadana i protecció de dades de caràcter personal. Finalment, atribueix al CCN la funció d'enllaç per garantir la cooperació transfronterera dels CSIRT de les administracions públiques amb els CSIRT internacionals, quan es tracti de la resposta als incidents i la gestió dels riscos de seguretat que els corresponen.

Vist l'anterior, és clar que el precepte objecte de dictamen, pel seu contingut i finalitat, s'insereix en l'àmbit de les competències sobre ciberseguretat, al qual ens hem referit en aquest mateix fonament jurídic i en el fonament jurídic tercer d'aquest Dictamen. I ho hem fet prenent com a punt de partida allò que vàrem exposar a bastament en el nostre Dictamen 5/2017 (FJ 2 i 3).

A tall de síntesi, recordarem alguns dels nostres raonaments allà exposats. Així, vàrem posar de manifest la importància de la seguretat en les diverses operacions que tenen lloc en el ciberespai, i vàrem precisar que els anomenats ciberatacs són accions que comprometen la disponibilitat, integritat i confidencialitat de la informació mitjançant l'accés no autoritzat, la modificació, la degradació o la destrucció dels sistemes d'informació i telecomunicacions o de les infraestructures que els donen suport. En aquest sentit, vàrem assenyalar que la «ciberseguretat» té diverses accepcions: d'una banda, presenta un aspecte directament relacionat amb l'autoprotecció de l'Administració de la Generalitat, que té com a finalitat última prevenir les amenaces i les vulnerabilitats inherents a les seves xarxes interdependents i infraestructures de la informació, tant internament com en les seves relacions amb els administrats i altres administracions o entitats públiques.

Recordem que la Generalitat té competències per a l'organització, el disseny, la creació i el manteniment dels serveis d'administració electrònica, ja que aquest és un aspecte fonamental de la potestat d'autoorganització que és inherent a l'autonomia (art. 150 i 159.1 EAC), com també té atribuïdes funcions executives per a la implementació de la convergència tecnològica i

la societat digital, i la protecció de les xarxes i els sistemes d'informació de l'Administració catalana i el seu sector públic, tant els propis com els dels particulars i els d'altres administracions que s'hi relacionen per mitjans electrònics. Des d'aquesta perspectiva, la Generalitat pot adoptar tot el ventall de mesures de protecció de la seguretat, de caràcter ordinari i preventiu que consideri necessàries, com també les que requereixi el restabliment de la normalitat dels sistemes (art. 140.7 EAC).

I, de l'altra, comprèn qüestions, igualment rellevants, que incideixen en àmbits connectats a les telecomunicacions i el règim general de comunicacions, la defensa i la seguretat pública (art. 149.1.4, .21 i .29 CE i art. 140.7 i 164 EAC) (DCGE 5/2017, FJ 2). D'aquesta manera, s'identifiquen amb la defensa militar i la seguretat nacional aquells supòsits de més gravetat, urgència i major dimensió, que poden afectar la prestació dels serveis essencials per a la ciutadania i la convivència social bàsica, i es connecten amb la seguretat pública els que tractin de la protecció de determinades infraestructures de telecomunicacions o de la investigació, prevenció i persecució de delictes. I, finalment, tenen relació amb les telecomunicacions els que es projecten sobre aspectes més tècnics que permetin assegurar el desplegament i l'efectivitat de les xarxes i, en general, de les tecnologies de la informació (DCGE 5/2017, FJ 2 i 3).

Per la seva part, també respecte de l'enquadrament competencial de la matèria de ciberseguretat com a sinònim de seguretat en la xarxa, el Tribunal Constitucional, a l'abans citada STC 142/2018, ha raonat que no existeix un títol competencial autonòmic específic respecte la matèria «ciberseguretat», i que «debe partirse del carácter transversal e interconectado de las tecnologías de la información y las comunicaciones y de su conceptuación como conjunto de mecanismos dirigidos a la protección de las infraestructuras informáticas y de la información digital que albergan los sistemas interconectados. Componente tuitivo al que se ha aludido ya y

que determina que las cuestiones discutidas en el presente recurso deban resolverse a partir de su encuadramiento material en el ámbito de la seguridad pública en relación con las telecomunicaciones y la seguridad nacional» (FJ 5).

Per tant, tal com hem dit en aquest fonament jurídic, l'Estat està habilitat per legislar sobre el règim general de comunicacions (art. 149.1.21 CE) en relació amb la protecció de la seguretat pública (art. 149.1.29 CE). Més encara, confrontant la seguretat nacional amb la ciberseguretat, ha romàs establert el vincle entre les competències de telecomunicacions i la seguretat nacional (STC 142/2018, FJ 4 a 6).

Finalment, en aquest mateix pronunciament, el Tribunal ha declarat que correspon a la Generalitat «adoptar medidas en materia de ciberseguridad en tanto en cuanto se aplican a las relaciones que tiene con sus administrados y con otras administraciones, así como respecto de las infraestructuras tecnológicas, que pertenezcan a la estructura de la Administración de la Generalitat y a su sector público» (FJ 4). I, referint-se a l'ACC, ha reconegut que la potestat d'autoprotecció comprèn, entre d'altres, les funcions «dirigidas a prevenir y mitigar los efectos de los ciberataques […], para lo que ha de ejercer las funciones de análisis, investigación y respuesta necesarios para restablecer sus propios servicios y garantizar su seguridad». I que, d'altra part, la dita funció «solo se lleva a cabo respecto de los sistemas de información, servicios de tecnologías de la información y la comunicación "en los que la Agencia intervenga por razón de su competencia"»; és a dir, com reitera al llarg del seu pronunciament, en relació amb la protecció exclusivament dels sistemes d'informació i comunicació de l'Administració de la Generalitat i el seu sector públic (FJ 7).

Pel que ara interessa, l'esmentada ACC, creada a l'empara de les competències d'autoorganització i provisió dels mitjans necessaris per a

l'exercici de les funcions de l'administració electrònica (art. 150 i 159.1 EAC), té atribuïda les funcions d'equip de resposta a emergències (CERT) competent a Catalunya, incloent-hi la relació amb altres organismes de ciberseguretat nacionals i internacionals, i la coordinació dels equips de resposta a incidents de ciberseguretat (CSIRT) i equips de resposta a emergències o entitats equivalents que actuïn en llur àmbit territorial (art. 2.4.*c* Llei 15/2017). Sobre aquesta qüestió, en el Dictamen tantes vegades citat vàrem dir que l'ACC exercirà aquestes funcions en l'àmbit de les competències de l'Administració de la Generalitat, amb els efectes territorials que preveu l'article 115 EAC. Per tant, és competent a Catalunya com a equip de resposta a les emergències que es produeixin, respectant sempre les facultats d'altres organismes estatals i supraestatals o internacionals, quan estiguin habilitats competencialment per actuar en el territori de Catalunya (aquest podria ser el cas, per exemple, del CCN-CERT, INCIBE-CERT o CERT-EU).

I així mateix, «quant a l'atribució de la funció de "coordinació dels equips a incidents de ciberseguretat (CSIRT) i equips de resposta a emergències o entitats equivalents que actuïn en llur àmbit territorial", s'ha d'entendre que únicament pot ser exercida en el marc de les seves competències estatutàriament assumides. És a dir, en relació amb els equips de resposta a ciberincidents o a emergències de l'Administració de la Generalitat i el seu sector públic, creats en els diferents àmbits sectorials i que afectin les persones físiques i jurídiques sobre les que pot actuar l'ACC» (DCGE 5/2017, FJ 3).

Arribats a aquest punt, hem de recuperar la idea de coordinació que presideix tot l'entramat de mecanismes orgànics i funcionals establerts per a la prevenció i resposta als incidents de ciberseguretat de les xarxes. Sobre aquesta qüestió, cal recordar que la «coordinació, en general, permet a l'Estat configurar una instància o un procediment de participació o bé establir

uns criteris de decisió que vinculen les comunitats autònomes, a fi d'assolir una orientació coherent en l'exercici de les competències respectives, però no pot substituir la decisió que correspon a cada una de les parts. El Tribunal Constitucional ha rebutjat sistemàticament que l'Estat pugui adoptar les decisions de caràcter substancial, i ha vinculat la coordinació a la fixació de mitjans i sistemes de relació que facin possible la informació recíproca, una certa homogeneïtat tècnica i l'acció conjunta de les autoritats (STC 148/2000, d'1 de juny, FJ 13.*d*), la qual cosa es coneix com a concepte adjectiu o processal de coordinació» (DCGE 15/2012, de 20 de novembre, FJ 2).

Respecte al principi de col·laboració entre administracions públiques per a l'exercici de les competències respectives en un determinat àmbit d'actuació, cal dir també, a tall de recordatori, que les fórmules racionals d'actuació conjunta (de cooperació, consulta, participació, concertació o acord) són fonamentals per a l'efectivitat del dit principi, que és inherent i consubstancial a l'Estat autonòmic, però «no poden servir per eludir responsabilitats pròpies ni per exercir les competències que el sistema constitucional ha atribuït a altres administracions» (per totes, STC 132/2018, de 13 de desembre, FJ 10, i 53/2017, d'11 de maig, FJ 16).

En els termes exposats, i atès que no es desprèn el contrari dels paràgrafs primer i segon del nou apartat 3 de l'article 7 RDL 13/2018, cap objecció es pot realitzar a la funció de coordinació dels CSIRT a nivell estatal atribuïda al CCN, com tampoc al mandat, dirigit indistintament als equips de resposta a incidents de ciberseguretat (CSIRT) de totes les administracions públiques, de consultar als òrgans amb competències específiques en matèria de seguretat nacional, seguretat pública, seguretat ciutadana i protecció de dades de caràcter personal i de col·laborar amb ells en l'exercici de les funcions atribuïdes a cadascun.

Quant a la funció d'enllaç, també atribuïda al CCN pel tercer i darrer paràgraf del mateix article 7.3, resulta de la transposició de la Directiva NIS que, com hem avançat, exigeix a cada Estat membre la designació d'un únic punt de contacte en matèria de seguretat de les xarxes i els sistemes d'informació per tal garantir la cooperació transfronterera entre les autoritats dels estats membres i amb les autoritats competents en altres estats membres i amb el grup de cooperació i la xarxa de CSIRT (art. 8, apts. 3 i 4). A més, els estats membres han de vetllar perquè els punts de contacte únic disposin de recursos adequats per exercir les seves funcions de forma eficient i efectiva i compleixin així amb els objectius establerts per la Directiva NIS (art. 8, apt. 5). En el cas que sigui procedent, tant els punts de contacte únic com les autoritats competents dels estats, d'acord amb el dret intern, consultaran les autoritats policials competents i les autoritats responsables de la protecció de dades i cooperaran amb elles (art. 8, apt. 6). A l'últim, els estats membres notificaran sense dilació a la Comissió el punt de contacte únic, la qual publicarà la llista de tots els designats (art. 8, apt. 7).

Sobre les relacions de la Generalitat amb la Unió Europea, hem de recordar que, amb caràcter general, la Generalitat participa, en els termes que estableixin l'Estatut i la legislació de l'Estat, en els afers amb els que tingui relació, que afectin les competències o els interessos de Catalunya (art. 184 EAC). Així mateix, la Generalitat aplica i executa el dret de la Unió Europea en l'àmbit de les seves competències, de tal manera que l'existència d'una regulació europea no modifica la distribució interna de competències que estableixen la Constitució i l'Estatut. En cas que l'execució del dret europeu requereixi l'adopció de mesures internes d'abast superior al territori de Catalunya que les comunitats autònomes competents no poden adoptar per mitjà de mecanismes de col·laboració o coordinació, l'Estat ha de consultar la Generalitat sobre aquestes circumstàncies abans que s'adoptin les dites mesures. Ultra això, la Generalitat ha de participar en els òrgans que adoptin

aquestes mesures o, si aquesta participació no és possible, ha d'emetre un informe previ (art. 189 EAC).

En el nostre DCGE 3/2011, de 24 de març (FJ 2), ja vàrem indicar que «el dret de la Unió Europea no és cànon de constitucionalitat per a la resolució dels conflictes de competència que es puguin produir al si de l'Estat espanyol. En efecte, el principi d'autonomia institucional reconegut per l'ordenament comunitari (art. 4.2 TUE) comporta dues conseqüències importants que convé no oblidar com són que l'execució i la transposició del dret comunitari les han de dur a terme precisament les institucions i els poders públics que disposen de la competència constitucional per fer-ho i, sobretot, que l'ordre constitucional i estatutari de competències no pot resultar modificat ni alterat per les disposicions del dret comunitari derivat». Ara bé, fent citació de la doctrina constitucional, vàrem dir que «"no cabe ignorar que la propia interpretación del sistema de distribución competencial entre el Estado y las Comunidades Autónomas tampoco se produce en el vacío" (STC 102/1995, de 26 de junio, FJ 5). Por ello, prestar atención a cómo se ha configurado una institución por la normativa comunitaria puede ser no sólo útil, sino incluso obligado para proyectar correctamente sobre ella el esquema interno de distribución competencial" (STC 33/2005, de 17 de febrer, FJ 4)».

Igualment, recentment, el Tribunal Constitucional, fent-se ressò d'una consolidada doctrina, ha afirmat que no existeix a la Constitució, ni als estatuts d'autonomia o al bloc de la constitucionalitat, una «"competencia específica" para la ejecución del Derecho comunitario» o «en general para el cumplimiento de los tratados internacionales válidamente celebrados por España […], sino que esa ejecución o cumplimiento "corresponde a quien materialmente ostente la competencia, según las reglas de Derecho interno"» (STC 87/2019, de 20 de juny, FJ 6).

Això anterior significa que l'Estat, en un principi, no pot emparar-se en la competència exclusiva sobre relacions internacionals (art. 149.1.3 CE) per estendre el seu àmbit competencial a qualsevol activitat que constitueixi desenvolupament, execució o aplicació del Dret derivat europeu. Ara bé, no es pot ignorar tampoc la necessitat de proporcionar al Govern estatal els instruments indispensables per exercir la funció que li atribueix l'article 93 CE, és a dir «"para adoptar las medidas necesarias a fin de garantizar el cumplimiento de las resoluciones de los organismos internacionales en cuyo favor se han cedido competencias… función que solo una interpretación inadecuada de los preceptos constitucionales y estatutarios puede obstaculizar». I l'anterior amb el benentès que, segons la distribució competencial afectada, principalment si es tracta de matèries compartides o concurrents entre l'Estat i les comunitats autònomes, l'exercici de les competències pròpies d'un i d'altres s'hagi d'articular sense envair l'àmbit competencial aliè (ibídem).

En el cas que ara ens ocupa, la designació d'un organisme com a punt d'enllaç únic de coordinació internacional està emparada per les competències de l'Estat en matèria de relacions internacionals (art. 149.1.3 CE) amb relació a les seves potestats exclusives sobre telecomunicacions, seguretat pública i defensa (art. 149.1, subapts. 4, 21 i 29 CE). Alhora, aquesta designació no és obstacle perquè les comunitats autònomes designin les seves pròpies autoritats públiques per vetllar per la seguretat de les xarxes i els sistemes d'informació que són de la seva competència, com tampoc exclou que estableixin els CSIRT que considerin necessaris, els quals formaran part de la xarxa de CSIRT creada per l'esmentada Directiva NIS.

Per tant, en conclusió, considerem que aquest precepte no evidencia causes d'inconstitucionalitat. I això és així, tal com es desprèn dels arguments que hem exposat, perquè l'Estat, a l'empara de les seves competències *ex* article 149.1.3 CE i en compliment de les obligacions assumides per aplicació del

dret europeu, ha de poder adoptar les mesures necessàries de coordinació a nivell intern però també amb els estats membres de la Unió i altres organismes europeus, en aquest cas per a la resposta als incidents i la gestió dels riscos de seguretat que corresponguin. Així, les autoritats i els serveis públics identificats per la legislació sectorial estatal corresponent són els responsables principals en les relacions de col·laboració i de cooperació amb d'altres estats.

Aquesta premissa, però, tampoc no impedeix que les lleis estatals puguin fixar en la seva normativa un model de col·laboració que reflecteixi la naturalesa composta del model constitucional i territorial espanyol. En aquesta línia, les lleis i les normes reglamentàries podrien incloure, per exemple, organismes —comissions, delegacions o grups de treball— i mecanismes i procediments de participació institucionals que integressin en l'àmbit estatal representants autonòmics. En el camp de la seguretat pública, destaca la previsió de l'article 164 EAC, el qual incorpora la potencial participació del cos de Mossos d'Esquadra en grups i delegacions internacionals, quan així ho prevegin —i en els termes en què ho facin— les lleis estatals corresponents. I, a la pràctica, a través dels sistemes digitals i de telecomunicacions, la policia catalana i també la basca tenen accés en l'actualitat, en diferents nivells, a bases de dades i mecanismes de cooperació europea i internacional.

Tanmateix, aquesta opció, com ja hem remarcat, que seria més plural i coherent amb un model autonòmic o federal, no està prevista com una exigència o un requisit de constitucionalitat de les lleis per part de la jurisprudència constitucional vigent, que interpreta la norma fonamental. En altres paraules, més sintètiques, una legislació estatal que prevegi la participació de les autoritats i els serveis públics autonòmics en les relacions de cooperació internacional és possible i ajustada a l'ordre constitucional però no és obligatòria a efectes de la seva adequació o validesa

constitucional. Per tant, és a l'àmbit polític i institucional a qui correspon fer viable aquesta mena d'alternatives reguladores, mitjançant la flexibilització de determinats elements que són configurats, com en el present cas, seguint un model centralitzat.

En conseqüència, i ja com a conclusió, l'article 7 RDL 14/2019, de 31 d'octubre, en el nou apartat 3 de l'article 11 RDL 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació, en la mesura que preveu un model basat en la col·laboració dels CSIRT de totes les administracions públiques amb els òrgans amb competències en seguretat pública i protecció de dades de caràcter personal, entre els quals s'inclouen els de la Generalitat, i que l'Estat, d'acord amb les seves competències *ex* article 149.1, subapartats 3, 21 i 29 CE, té potestat per designar un punt de contacte únic, a l'efecte de la coordinació transfronterera per al compliment de les obligacions de la Directiva 2016/1148, de 6 de juliol (art. 8), no vulnera les competències de la Generalitat previstes als articles 140.7, 159.1 i 164 EAC.

Cinquè. L'examen de constitucionalitat i d'estatutarietat dels preceptes del Reial decret llei 14/2019 relatius a la protecció de dades personals

En aquest fonament jurídic tractarem els preceptes del capítol II del Reial decret llei que regulen aspectes relatius a la protecció de dades personals i que han estat qüestionats pel sol·licitant. En concret, l'article 3, apartats u i dos, RDL 14/2019, que introdueixen un nou apartat 3 als articles 9 i 10 LPACAP i el seu règim transitori (disp. trans. primera, apt. 2 RDL 14/2019); l'article 4, apartat u, que incorpora l'article 46 bis a la LRJSP i el seu règim transitori (disp. trans. segona RDL 14/2019), i l'article 4, apartat dos, que dona una nova redacció a l'article 155 d'aquesta darrera Llei.

Segons la disposició final primera, els articles 3 i 4 RDL 14/2019 es dicten a l'empara de les clàusules competencials núm. 18 i 29 de l'article 149.1 CE, per bé que no identifica quines de les mesures regulades s'empararien en cadascun dels títols, tenint en compte que aquests tenen un abast i uns efectes diferents. Nogensmenys, del preàmbul de la norma sembla desprendre's que les previsions objecte d'examen en aquest fonament jurídic es troben principalment fonamentades en la competència exclusiva estatal sobre seguretat pública (llevat de l'art. 4.dos). Caldrà, doncs, amb ocasió del seu examen, delimitar quin és el paràmetre competencial aplicable.

1. Abans, però, convé efectuar algunes consideracions generals sobre la matèria de la protecció de les dades personals, atès que és subjacent a tots els preceptes ara examinats en la mesura que afectin qualsevol informació sobre una persona física identificada o identificable.

Així, quant al seu context normatiu i de forma sintètica, cal fer referència a la seva primera regulació internacional, inspiradora de la normativa europea posterior, mitjançant el Conveni núm. 108 del Consell d'Europa per a la protecció de les persones amb respecte al tractament automatitzat de dades de caràcter personal, obert a Estrasburg per a la seva signatura el 28 de gener de 1981 i ratificat per l'Estat espanyol en data de 27 de gener de 1984 (BOE núm. 274, de 15 de novembre de 1985), el qual ha estat modificat recentment mitjançant el Protocol de 10 d'octubre de 2018, que l'ha actualitzat i ha aprovat una nova versió del Conveni (signada també per l'Estat espanyol) després de més de tres dècades de vigència de l'anterior (Conveni 108+).

A escala europea, l'article 16.1 del Tractat de funcionament de la Unió Europea (en endavant, TFUE) reconeix el dret de la persona a la protecció de les dades de caràcter personal que el concerneixin, com també ho fa l'article

8.1 de la Carta de drets fonamentals de la Unió Europea, formalment proclamada a Niça el 7 de desembre de 2000. En el marc d'aquestes normes, s'adopta el Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en allò que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades [en endavant, Reglament (UE) 2016/679 o RGPD], que ha derogat la Directiva 95/46/CE del Parlament Europeu i del Consell, de 24 d'octubre de 1995, la qual va tenir en el seu moment una importància cabdal en l'àmbit que ara ens ocupa. Aquest panorama normatiu es completa amb la Directiva (UE) 2016/680 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relativa a la protecció de les persones físiques en allò que respecta al tractament de dades personals per part de les autoritats competents per a finalitats de prevenció, investigació, direcció o enjudiciament d'infraccions penals o d'execució de sancions penals, i a la lliure circulació d'aquestes dades.

La nostra atenció se centra en l'esmentat Reglament (UE) 2016/679, que té per objecte dues finalitats principals: d'una banda, l'establiment de les normes relatives a la protecció dels drets i les llibertats de les persones físiques pel que respecta al tractament de les dades personals i, de l'altra, les referides a la lliure circulació de les dades personals dins de la Unió, la qual no podrà ser restringida ni prohibida, quant al seu tractament, en supòsits diferents als que preveu o possibilita el Reglament mateix (art. 1). Així, se cerca un equilibri entre la protecció dels ciutadans i la llibertat d'iniciativa econòmica, com també de la cooperació entre estats. Certament, molts dels principis i fonaments de la Directiva 95/46/CE segueixen actius però hom pot dir que el Reglament europeu, que fixa amb més precisió el dret fonamental a la protecció de dades, opera un canvi de model que, sintèticament, passa de la gestió de les dades a l'ús responsable de la informació. Això es tradueix en nous principis com el de la responsabilitat proactiva (art. 5.2 i 24), el consentiment exprés del titular de les dades com

a base de legitimació del tractament (art. 4.11 i 7), el nou dret a la portabilitat (art. 20), la privacitat des del disseny i per defecte (art. 25), la protecció de les dades basada en l'anàlisi de riscos i les mesures de seguretat adequades a aquests (art. 32), l'avaluació d'impacte (art. 35), la figura del delegat de protecció de dades (art. 37), la importància dels codis de conducta (art. 40), el registre d'activitats del tractament (art. 30), l'enfortiment del paper de les autoritats de control dels estats membres (art. 51 a 59), inclòs el del Comitè Europeu de Protecció de Dades (art. 68 a 76), que contribueix a l'aplicació coherent de les normes de protecció de dades a tota la Unió Europea i promou la cooperació entre les esmentades autoritats, o el règim de recursos, responsabilitat i sancions (art. 77 a 84).

En una línia seqüencial semblant, a nivell intern, s'han aprovat diverses lleis i normes de desenvolupament en la matèria de protecció de dades personals, fins a arribar a la vigent Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (en endavant, LOPDGDD), que ha derogat la precedent Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.

Atès l'anterior, cal referir-se amb caràcter previ a la naturalesa i els efectes del Reglament (UE) 2016/679, el qual és d'aplicació obligatòria des del 25 de maig de 2018. Des d'una perspectiva formal, es tracta d'una norma amb un abast general, que és obligatòria en tots els seus elements i directament aplicable a tots els estats membres (art. 288 TFUE). Per tant, no requereix transposició o desenvolupament mitjançant normes internes i comporta el desplaçament de les que esdevinguin incompatibles amb ella. És clar que la seva adaptació pot exigir l'adopció de noves disposicions internes que complementin o esclareixin el seu contingut, però únicament amb la finalitat d'assegurar l'efecte útil del que disposa i sense induir a errada sobre la seva naturalesa i aplicabilitat directa.

El Reglament europeu mateix declara que pretén establir un marc més sòlid i coherent (considerant 7), que eviti una aplicació fragmentada, la inseguretat jurídica i les diferències en la protecció dels drets i llibertats en els estats membres (considerant 9) i que garanteixi un nivell uniforme i elevat de protecció (considerant 10). Cal assenyalar que també conté nombroses remissions d'abast variable al dret dels estats membres que permet a aquests adaptar-ne la regulació, en distints supòsits, al context estatal; o a fixar exempcions, limitacions o derogacions o condicions específiques per a determinades categories de tractament de dades, o, fins i tot, en alguns casos puntuals el Reglament confereix caràcter preceptiu a aquesta tasca normativa de desenvolupament. Altrament, es reconeix amb caràcter general un marge de maniobra perquè els estats membres especifiquin les seves normes (considerant 10) i la possibilitat que mantinguin o introdueixin disposicions més específiques per adaptar l'aplicació de les prescripcions del Reglament, tot establint de forma més precisa requisits concrets per al tractament de dades personals amb altres finalitats, prenent en consideració l'estructura constitucional, organitzativa i administrativa de l'Estat membre en concret. Ara bé, aquesta limitació ha de constituir una mesura necessària i proporcionada en una societat democràtica per protegir interessos específics importants, entre ells, la seguretat pública i la prevenció, la investigació, la detecció i l'enjudiciament d'infraccions penals o d'execució de sancions penals (considerant 19).

Amb relació a la naturalesa del Reglament (UE) 2016/679, el Tribunal Constitucional ha recordat que la seva eficàcia jurídica no s'esgota en el «valor hermenéutico que despliega a los efectos del artículo 10.2 CE, esto es, en el plano de la constitucionalidad» sinó que en el «seno de nuestro ordenamiento jurídico representa sobre todo un acto jurídico "obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro", como luce al final del texto y con las características inherentes al Derecho de la Unión Europea» (STC 76/2019, de 22 de maig, FJ 3).

D'aquesta manera, tot i que reitera que no constitueix paràmetre de constitucionalitat, afegeix que quan es tracta de l'enjudiciament constitucional del desenvolupament legislatiu d'un dret fonamental com és la protecció de dades personals, que es troba parcialment determinat pel dret de la Unió Europea, les exigències que deriven d'aquest darrer «no pueden ser irrelevantes a la hora de establecer los márgenes constitucionalmente admisibles de libertad de apreciación política» (STC 1/2012, de 13 de gener, FJ 9). Altrament, una eventual conclusió d'incompatibilitat entre una llei interna i una disposició del dret de la Unió Europea s'ha de dirimir «en términos de legalidad ordinaria y selección del derecho aplicable en un primer término, y no en clave de contradicción con la Constitución» (STC 76/2019, de 22 de maig, FJ 3, fent cita de la STC 140/2018, de 20 de desembre, FJ 6).

Cal tenir present, per a una correcta anàlisi dels preceptes sol·licitats, que el règim jurídic del tractament de dades de caràcter personal està previst tant en el Reglament (UE) 2016/679 com en la LOPDGDD, ja que ambdues fonts normatives configuren conjuntament, de forma directa o supletòria, el desenvolupament del dret fonamental a la protecció de dades de caràcter personal que exigeixen els articles 18.4 i 81.1 CE (art. 1.*a* i 2 LOPDGDD i art. 2 i 3 RGPD).

Arribats a aquest punt i tenint present la seva evident evolució, ens hem de referir sintèticament al dret fonamental a la protecció de dades i al seu contingut essencial segons l'ha configurat la doctrina constitucional. Aquest dret, que neix de l'article 18.4 CE, independentment del dret a la intimitat i amb singularitat pròpia, atribueix al seu titular un poder de control i de disposició de les seves dades personals, automatitzades o no, que es fa efectiu mitjançant la imposició de deures o obligacions a tercers. Així, faculta la persona per decidir quines dades vol proporcionar a un tercer, sigui un

poder públic o un particular, o quines pot recaptar aquest tercer, com també li permet saber i ser informat respecte de qui les posseeix i per a què les vol, de manera que es pot oposar a aquesta possessió o a aquest ús.

En altres paraules, els esmentats poders de control i de disposició que constitueixen part del contingut nuclear del dret fonamental a la protecció de dades, es concreten jurídicament en la facultat de consentir la recollida, l'obtenció i l'accés a les dades personals, el seu posterior emmagatzematge i tractament, i el seu ús o usos possibles per un tercer. Dit això, cal afegir que l'article 18.4 CE té dues vessants, com a dret fonamental autònom que s'ha descrit, que permet a l'individu controlar el flux de les informacions relatives a la seva persona, i com a dret fonamental instrumental orientat a la protecció o garantia d'altres drets fonamentals, com són els drets a la intimitat i a l'honor o a la llibertat ideològica (per totes, STC 292/2000, de 30 de novembre, FJ 6, i, més recentment, STC 76/2019, FJ 5).

Finalment, s'ha d'assenyalar que, per preservar i possibilitar l'exercici del ventall de facultats que integren el contingut essencial del dret a la protecció de dades, el legislador ha d'establir les «garanties adequades» de tipus tècnic, organitzatiu i procedimental que el protegeixin de manera eficaç. I l'anterior amb el benentès que la necessitat i l'abast de les garanties pot diferir força segons el tipus de tractament que es pretén dur a terme, la naturalesa mateixa de les dades (són més exigibles i específiques quan es tracta de categories especials de dades) i la probabilitat i la gravetat dels riscos d'abusos i d'accés o utilització il·lícits (STC 76/2019, FJ 6, fent citació de jurisprudència de la doctrina del TJUE).

Dit això, s'ha d'indicar que, en la delimitació del dret fonamental de protecció de dades, el legislador estatal haurà d'harmonitzar la reserva de llei orgànica relativa al seu contingut essencial (art. 81.1 CE) amb la possibilitat d'un ulterior desenvolupament en els diferents àmbits materials en els quals es

projecti el seu exercici, que es regiran per les regles de la distribució constitucional i estatutària de competències que deriven de l'article 149.1 CE. En aquest sentit, la doctrina constitucional recorda que l'article 81.1 CE, que no és un títol atributiu de competències sinó un precepte ordenador del sistema de fonts, no pot desvirtuar allò que disposa l'article 149.1 CE sobre l'articulació dels àmbits materials corresponents a l'Estat i les comunitats autònomes i, per tant, ha de cohonestar-se amb el bloc de la constitucionalitat. D'acord amb l'anterior, ha declarat que l'àmbit reservat a la llei orgànica, que s'ha d'interpretar restrictivament, comprèn el desenvolupament directe del dret fonamental considerat en abstracte «en cuanto tal» mentre que la regulació de la «materia» sobre la qual es projecta el dret s'atribueix al legislador ordinari, estatal o autonòmic, amb competències sectorials sobre aquella (per totes, STC 135/2006, de 27 d'abril, FJ 2).

2. Fetes les consideracions anteriors, a continuació examinarem els apartats u i dos de l'article 3 RDL 14/2019, que afegeixen als articles 9 i 10 LPACAP nous i sengles apartats 3, amb els següents continguts:

Article 9 LPACAP:

> «3. En relació amb els sistemes d'identificació que preveu la lletra c) de l'apartat anterior, s'estableix l'obligatorietat que els recursos tècnics necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió d'aquests sistemes estiguin situats en territori de la Unió Europea, i en territori espanyol en cas que es tracti de categories especials de dades a què es refereix l'article 9 del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE. En tot cas, les dades han d'estar disponibles perquè hi puguin accedir les autoritats judicials i administratives competents.

> Les dades a què es refereix el paràgraf anterior no poden ser objecte de transferència a un tercer país o organització internacional, a excepció dels que hagin estat objecte d'una decisió d'adequació de la Comissió Europea o quan així ho exigeixi el compliment de les obligacions internacionals assumides pel Regne d'Espanya.»

Article 10 LPACAP:

> «3. En relació amb els sistemes de signatura que preveu la lletra c) de l'apartat anterior, s'estableix l'obligatorietat que els recursos tècnics necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió d'aquests sistemes estiguin situats en territori de la Unió Europea, i en territori espanyol en cas que es tracti de categories especials de dades a què es refereix l'article 9 del Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016. En tot cas, les dades han d'estar disponibles perquè hi puguin accedir les autoritats judicials i administratives competents.
>
> Les dades a què es refereix el paràgraf anterior no poden ser objecte de transferència a un tercer país o organització internacional, a excepció dels que hagin estat objecte d'una decisió d'adequació de la Comissió Europea o quan així ho exigeixi el compliment de les obligacions internacionals assumides pel Regne d'Espanya.»

A) Com es pot constatar, es tracta de dues previsions normatives d'idèntic contingut, que s'apliquen específicament i concreta als sistemes validats per les administracions públiques d'identificació electrònica dels administrats, anomenats de clau concertada i altres (art. 9.2.*c* LPACAP) i de signatura diferents als de signatura electrònica qualificada i avançada (art. 10.2.*c* LPACAP) als quals hem fet referència a bastament en el fonament jurídic tercer.

Pel que ara ens interessa, les normes transcrites adopten les següents mesures: d'una banda, estableixen l'obligació legal que «els recursos tècnics

necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió d'aquests sistemes estiguin situats en el territori de la Unió Europea». En cas que es tracti de categories especials de dades, els dits recursos han d'estar localitzats «en territori espanyol».

A aquests efectes, segons l'article 9 RGPD, que se cita en el text de les normes objecte de dictamen, estan incloses en les categories especials de dades les que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques o l'afiliació sindical, i el tractament de dades genètiques, dades biomètriques dirigides a identificar de manera unívoca una persona física, dades relatives a la salut o dades relatives a la vida sexual o l'orientació sexual d'una persona física. Aquestes dades, atesa la seva naturalesa, són particularment sensibles i, consegüentment, el Reglament (UE) 2016/679 en prohibeix el seu tractament com a principi, si bé aquesta regla general s'exceptua en situacions específiques com, per exemple, quan l'interessat hi doni el seu consentiment explícit o sigui necessari per protegir els seus interessos vitals i es trobi incapacitat per consentir (art. 9).

I, de l'altra, contenen la prohibició de transferència internacional de les dades a un tercer país o a una organització internacional, llevat de dos supòsits: que aquests hagin estat objecte d'una decisió d'adequació de la Comissió Europea o quan així ho exigeixi el compliment de les obligacions internacionals assumides per Espanya. A l'últim, prescriu que les dades tractades han d'estar disponibles perquè hi puguin accedir autoritats judicials i administratives.

El sol·licitant es qüestiona si les limitacions territorials a l'hora d'ubicar els recursos tècnics comporten una ingerència en les competències de la Generalitat que podrien esdevenir contràries als articles 150 i 159 EAC en tant que l'afecten «en l'organització dels serveis de la seva competència

quan els presta de forma directa», com també es planteja si poden ser constitutives «d'una vulneració de la lliure prestació de serveis i d'establiment que han de garantir la mobilitat de les empreses i els professionals a tota la Unió Europea, article 26 (mercat interior), 49 a 55 (establiment) i 56 a 62 (serveis) del Tractat de funcionament de la Unió Europea». A més, respecte de la limitació de les transferències internacionals, entén que restringeix «la possibilitat d'utilitzar altres mecanismes previstos a l'article 46 RGPD».

B) Per a una correcta anàlisi de les mesures ara examinades, que estan connectades entre si, començarem pels darrers paràgrafs dels nous apartats 3 dels articles 9 i 10 LPACAP, que estableixen la prohibició de realitzar transferències de dades a un tercer país o a una organització internacional, llevat que es tracti d'algun dels dos supòsits següents: quan hagin estat objecte d'una decisió d'adequació de la Comissió Europea o quan així ho exigeixi el compliment de les obligacions internacionals assumides pel Regne d'Espanya.

Abans de tot, però, cal determinar a quines dades s'aplicaria aquesta limitació de les transferències internacionals, ja que la norma no és gens clara des del moment que l'expressió «les dades a què es refereix el paràgraf anterior» pot comprendre les que s'inclouen en categories especials (esmentades expressament) però també altres dades d'identificació susceptibles de ser tractades pels sistemes electrònics d'identificació i signatura objecte de la regulació (art. 9.2.*c* i 10.2.*c* LPACAP). De la literalitat del precepte i de la seva interpretació conjunta amb el preàmbul del Reial decret llei (apt. II, par. setè) sembla desprendre's que la restricció de les transferències només s'aplicaria a les categories especials de dades previstes a l'article 9 RGPD i així ho considerarem en la nostra anàlisi.

Esclarit l'anterior, i per tal de contextualitzar la restricció explicitada, cal referir-se, ni que sigui molt breument, al concepte de transferència internacional i a la seva regulació actual en la normativa europea (art. 44 a 50 RGPD) i estatal (art. 40 a 43 LOPDGDD) per, tot seguit, enquadrar els preceptes en la matèria competencial que els correspon, atès el seu contingut i la seva finalitat.

La transferència internacional de dades no està explícitament definida a l'article 44 RGPD (tampoc ho feia la Directiva 95/46/CE) ni a la LOPDGDD, i el mateix Tribunal de Justícia de la Unió Europea tampoc no n'ha elaborat una definició formal sinó que ha delimitat aquest concepte en sentit negatiu (STJUE de 6 de novembre de 2003*,* assumpte *Lindqvist*, C-101-01). Així, ha raonat que la publicació en una pàgina web de dades personals emmagatzemada pel seu proveïdor de serveis d'allotjament domiciliat en territori de la Unió Europea a la qual es pot accedir des de qualsevol lloc, tot i que és un tractament, no és una transferència internacional de dades. Ho argumenta sobre la base que no implica una transmissió directa de dades entre dos subjectes, sinó que les dades personals que arriben a l'ordinador d'una persona que es troba en un país tercer i que procedeixen d'una persona que els ha publicat a internet, s'han transmès amb l'ajuda de la infraestructura informàtica del proveïdor de serveis d'allotjament de pàgines web on aquella està allotjada. En conseqüència, declara que no existeix una «transferència de dades a un país tercer» quan una persona que es troba en un Estat membre difon dades personals en una pàgina web, emmagatzemada pel seu proveïdor de serveis d'allotjament de pàgines web que té el seu domicili en el mateix Estat o en un altre Estat membre, de manera que les dites dades són accessibles per a qualsevol persona que es connecti a internet, incloses les que es troben en països tercers (apts. 61 i 71).

Resulta obvi que la determinació d'aquest concepte és, a la pràctica, complexa, atesos els nombrosos mitjans electrònics i intermediaris que actuen en aquest procés de transferència, però, simplificadament, es pot entendre com el flux de dades que suposa una transmissió d'aquestes per una persona física o jurídica, pública o privada, o un òrgan o entitat administratius situats en territori espanyol a un país tercer o a una organització internacional que es troben fora del territori de l'Espai Econòmic Europeu o EEE, que inclou els estats membres de la Unió Europea més Islàndia, Liechtenstein i Noruega (en aquest sentit, art. 5.1.*s* RD 1720/2007, de 21 de desembre, pel que s'aprovava el Reglament de la LOPD, vigent en allò que no s'oposi al RGPD i a la LOPDGDD), amb la finalitat última de tractar aquesta informació un cop hagi estat rebuda pel destinatari. O, també, es podria definir com aquell acte mitjançant el qual el transmitent permet el coneixement de les dades personals al destinatari de forma directa, implicant, per tant, una comunicació material de dades personals, amb independència de la seva finalitat, i essent internacional quan el lloc de destinació de les dades es localitza fora de l'espai de nivell adequat o equiparable de protecció (en aquest cas, fora de l'EEE). S'ha d'assenyalar que la referència a les organitzacions internacionals com a destinatàries de les transferències és una novetat del Reglament europeu.

Dit això, la transferència internacional de dades constaria dels següents elements: ha de tractar-se de dades que permetin identificar o fer identificable una persona de manera directa o indirecta; les dades personals poden ser tractades de forma automatitzada o no, o sigui, tant poden ser objecte de transmissió per mitjans informatitzats com per mitjans convencionals; la finalitat de la transferència és que el destinatari efectuï un tractament de les dades, ja sigui la seva cessió o comunicació (a un altre responsable) o la prestació d'un servei (encarregat del tractament), i, a l'últim, ha de tenir lloc un trasllat físic i efectiu de les dades d'un indret del

territori de l'EEE a un Estat o una organització internacional fora d'aquest, que esdevé el lloc de destinació.

Donat que les dades personals de ciutadans europeus situats en la Unió Europea són accessibles des de fora de l'EEE, l'objectiu primordial que persegueix el Reglament (UE) 2016/679 quan regula aquesta figura és garantir que quan es transfereixin a tercers països es mantingui un nivell de protecció adequat i conforme amb l'estàndard mínim que s'estableix en el seu articulat. El principi general és, doncs, que només es pot efectuar una transferència internacional de dades si el destinatari compleix amb totes les obligacions relatives al tractament que estableix la normativa europea aplicable i assegura les garanties suficients a l'hora de realitzar la transferència i, sobretot, en possibles i ulteriors transferències que pugui fer (considerant 101 i art. 44 RGPD). Ara bé, aquest objectiu ha de trobar un equilibri amb la preservació d'altres interessos com el fet que el flux de dades a tercers països afavoreix l'expansió del comerç internacional i la cooperació internacional en matèria de seguretat i prevenció dels delictes (considerants 1 i 101 RGPD i 7 Directiva 2016/680). Per la seva part, el Conveni 108+ imposa la regla general del lliure moviment de dades entre les parts contractants sempre que es tracti d'estats que disposin de normes harmonitzades sobre aquesta matèria (art. 14).

Vist aquest principi general, el Reglament (UE) 2016/679 admet la transferència internacional de dades només en els següents supòsits:

a) Quan es basi en una decisió d'adequació de la Comissió Europea que, per dir-ho molt sintèticament, és un acte jurídic emès per aquesta en què, a partir de l'anàlisi d'un seguit de condicions i requisits, es certifica que l'estat o organització internacional destinatari té un nivell de protecció adequat de les dades personals o substancialment equivalent al de la normativa europea (art. 45 RGPD). Actualment, els estats sobre els quals existeix una decisió

d'adequació vigent són: Suïssa (Decisió 2000/518/CE, de 26 de juliol), Canadà (Decisió 2002/2/CE, de 20 de desembre), Argentina (Decisió 2003/490/CE, de 30 de juny), Guernsey (Decisió 2003/821/CE, de 21 de novembre), Illa de Man (Decisió 2004/411/CE, de 28 d'abril), Jersey (Decisió 2008/393/CE, de 8 de maig), Illes Fèroe (Decisió 2010/146/CE, de 5 de març), Andorra (Decisió 2010/625/UE, de 19 d'octubre), Israel (Decisió 2011/61/UE, de 31 de gener), Uruguai (Decisió 2012/484/UE, de 21 d'agost), Nova Zelanda (Decisió 2013/65/UE, de 19 de desembre), Japó (Decisió d'execució 2019/419, de 23 de gener) i, amb singularitats pròpies, els Estats Units d'Amèrica (Decisió 2016/1250/UE, de 12 de juliol, aplicable a les entitats d'aquest país certificades en el marc del *Privacy Shield* UE-EUA).

b) Quan es basi en garanties adequades i a condició que els interessats comptin amb drets exigibles i accions legals efectives, dels quals cal informar l'interessat (art. 46 RGPD). Aquestes garanties es divideixen en dos blocs, segons si requereixen autorització expressa de l'autoritat de control o no. D'una banda, no cal autorització en el cas que les garanties s'aportin mitjançant un instrument jurídicament vinculant i exigible entre autoritats o organismes públics; normes corporatives vinculants, conegudes com *Binding Corporate Rules* o BCR (art. 47 RGPD); clàusules tipus de protecció de dades adoptades per la Comissió o bé per una autoritat de control i aprovades per la Comissió; codis de conducta, o mecanismes de certificació (art. 46.2 RGPD). I, de l'altra, ha d'existir l'autorització prèvia de l'autoritat de control quan s'aportin mitjançant clàusules contractuals acordades entre l'exportador i el destinatari de les dades o mitjançant disposicions que s'incorporin en acords administratius entre les autoritats o els organismes públics que incloguin drets efectius i exigibles per als interessats (art. 46.3 RGPD).

Cal indicar que la transferència internacional sobre la base del compliment d'una obligació internacional, que seria un altre supòsit admès, està prevista en el considerant 102 del Reglament (UE) 2016/679 i no pas en el seu

articulat. En aquest sentit, hem d'assenyalar que aquesta transferència s'ha de dur a terme respectant el conjunt de previsions que conté aquesta norma europea en la seva part dispositiva.

Nogensmenys, seguidament, el mateix Reglament (UE) 2016/679 admet un ventall d'excepcions per a situacions específiques, en llista tancada o *numerus clausus* (entre d'altres, quan sigui necessària per raons importants d'interès públic, exercici o defensa de reclamacions, o es realitzi des d'un registre públic), que, a més dels casos anteriors, permeten la transferència internacional de dades sense autorització de les autoritats de control, sempre que l'exportador d'aquestes garanteixi als interessats drets exigibles i efectius respecte al tractament de les seves dades (art. 49 i considerant 114 RGPD). Algunes d'aquestes excepcions no són aplicables a les administracions públiques en exercici de poders públics (art. 49.1, par. primer, lletres *a*, *b*, *c*, d'acord amb l'art. 49.3 RGPD) i són d'abast força ampli, des del moment en què s'accepten perquè obeeixen a interessos legítims imperiosos (art. 49.1, segon par., RGPD).

Consegüentment, exposat l'anterior, es pot dir que, de fet, el Reglament (UE) 2016/679 és força més permissiu que la normativa espanyola anterior a l'hora d'admetre les transferències internacionals i amplia els casos en què estan permeses, per bé que les envolta de les cauteles i garanties corresponents.

Per la seva part, la LOPDGDD, a l'hora de regular les transferències internacionals de dades, es remet al que disposa el Reglament (UE) 2016/679, a allò que ella mateixa determina en el seu articulat, a les normes de desenvolupament aprovades pel Govern i a les circulars de les autoritats estatal i autonòmiques de protecció de dades, en l'àmbit de les seves respectives competències (art. 40). Quant a l'articulat orgànic, es refereix a les especialitats relacionades amb procediments mitjançant els quals les

autoritats de control poden aprovar models contractuals o BCR, i als supòsits que requereixen autorització o informació prèvies d'una determinada transferència (art. 41 a 43).

Als efectes d'aquest Dictamen, cal destacar la previsió de l'apartat 5 de l'article 49 RGPD, que conté una habilitació específica perquè els estats membres puguin restringir les transferències internacionals més enllà del que disposa el Reglament europeu. Així, declara que, en el cas que no hi hagi una decisió per la qual es constati l'adequació de la protecció de les dades, aquells estan facultats per establir límits a la transferència de categories específiques de dades a un tercer país o organització internacional. Ara bé, sotmet aquesta potestat a dos requisits: la limitació ha d'estar fonamentada en «raons importants d'interès públic» i les disposicions que es dictin en aquest sentit han de ser notificades a la Comissió. Sobre l'abast d'aquesta norma res no aporta el considerant 112 RGPD que, simplement, l'enuncia.

Tenint en compte la normativa europea exposada, ens pertoca aplicar el paràmetre de constitucionalitat, amb la finalitat de poder concloure la seva adequació a la norma fonamental i, si escau, al Reglament europeu.

Com a qüestió prèvia, farem una breu referència a l'eventual reserva de llei orgànica *ex* article 81 CE. Un cop examinat el contingut de la mesura que ens ocupa, es pot dir que, atès que no desenvolupa el concepte mateix de transferència internacional de dades amb caràcter general, no constitueix un desenvolupament directe del contingut essencial del dret fonamental de l'article 18.4 CE, reservat a la llei orgànica, sinó que és una regulació sectorial que singularitza la qüestió de les transferències internacionals en la gestió de determinats sistemes d'informació i comunicació de les administracions públiques i, en última instància, afecta la manera en què aquestes poden organitzar la gestió dels dits serveis.

En vista d'aquesta darrera premissa, hem d'identificar quina seria la finalitat de la norma que estem analitzant per posar-la en relació amb la seva dimensió competencial i així poder determinar si l'Estat compta amb l'habilitació per dictar la mesura o, si per contra, afecta les competències organitzatives de l'Administració pública de la Generalitat.

Tal com hem indicat a l'inici d'aquest apartat, la norma introdueix una restricció a les transferències internacionals de dades, respecte d'un determinat tipus d'aquestes, les de categoria especial, i en relació amb uns concrets sistemes d'identificació dels interessats davant de les administracions públiques (clau concertada i altres) i de signatura electrònica (diferent als de signatura electrònica qualificada i avançada basada en certificats electrònics qualificats de firma electrònica).

D'acord amb el seu contingut, per tant, entenem que ens situem en el marc de les competències compartides relatives a les bases del règim jurídic de les administracions públiques i del procediment administratiu, configurat pels articles 149.1.18 CE i 159.1.*a* i .*c* EAC i, en connexió, per raó de la seva finalitat última, amb la protecció de la ciberseguretat. Aquesta darrera matèria, segons la dimensió que adquireixi, pot remetre també als títols dels articles 149.1.29 CE i 164 EAC, en els termes en què els hem descrit en els fonaments jurídics tercer i quart.

D'entrada, hem d'assenyalar que la iniciativa reguladora de reforçar les garanties de seguretat en el tractament de la categoria especial de dades, que és susceptible d'afectar un dret fonamental de les persones, tenint en compte el seu contingut, constitueix una finalitat legítima per part del legislador estatal que respon a un interès públic. Les dades relatives a qüestions significativament sensibles (com és el cas que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques o l'afiliació sindical, i el tractament de dades genètiques, dades biomètriques

dirigides a identificar de manera unívoca una persona física, dades relatives a la salut o dades relatives a la vida sexual o l'orientació sexual d'una persona física) són, com resulta evident, dignes d'una protecció reforçada per raó de l'interès públic consistent en la garantia de l'*habeas data* dels ciutadans. Aquesta protecció ampliada troba encaix tant en les previsions del Reglament europeu, que les facilita a través del règim d'excepcions justificades (considerants 51 i seg. i art. 9.4 RGPD), com en el cànon de constitucionalitat i d'estatutarietat aplicable.

Respecte de l'ordre constitucional espanyol, aquest Consell considera que, d'una banda, la regulació objecte de dictamen no exigeix la reserva de llei orgànica, atès que no desenvolupa ni afecta de forma directa el nucli essencial del règim jurídic d'un dret fonamental, en aquest cas, la protecció de dades *ex* article 18.4 CE. I, de l'altra, que la mesura consistent a incrementar el nivell de seguretat d'aital dret en aquest concret aspecte, per la via de la limitació de la seva transferència internacional, troba aixopluc en les competències estatals en matèria de règim jurídic de les administracions públiques i de procediment comú (art. 149.1.18 CE).

En aquest sentit, creiem que les competències de la Generalitat no es veuen vulnerades, perquè el que esdevé rellevant a l'efecte del seu suport constitucional és el fet que el legislador estatal prescriu la seguretat i garantia de determinades dades per raó del seu contingut altament sensible, amb independència de si es vinculen o van aparellades amb un tipus d'identificació i signatura electrònica d'operativa autonòmica. En conseqüència, la finalitat perseguida és la igualtat dels ciutadans en l'àmbit material de les relacions amb les administracions públiques. I no hi ha gaire espai al dubte quan s'argumenta que tots els ciutadans de l'Estat poden ser emparats per una legislació bàsica que els garanteix que les seves dades, susceptibles d'identificar la seva esfera religiosa, sexual, mèdica o política, no poden ser transferides fora de l'espai assegurat pel Reglament europeu,

llevat que hagin estat objecte d'una decisió d'adequació de la Comissió Europea o quan així ho exigeixi el compliment de les obligacions internacionals assumides per l'Estat espanyol.

Aquesta restricció incorporada per la llei estatal respon, segons el nostre parer, a un interès públic, i no és desproporcionada fins al punt de contravenir la normativa europea, en la mesura que compatibilitza una finalitat legítima amb el respecte al sistema general de transferències internacionals habilitat per la normativa europea (art. 49.5 RGPD) i, per la seva banda, troba inserció en el contingut de les bases estatals en règim jurídic de les administracions i procediment comú quant a la posició igualitària dels ciutadans davant de les administracions públiques.

La Generalitat, en tot cas, pot articular el seu sistema o model d'administració electrònica, amb el marge que li atribueixen els articles 159.1.*a* i .*c* EAC, però respectant i tenint cura que les dades de categoria especial no poden ser transmeses a tercers països, externs a l'EEE, si aquests no són titulars d'una decisió d'adequació de la Comissió Europea o l'operació no ve suportada per una obligació internacional degudament contreta. Un marc, aquest, que entenem que permet compatibilitzar l'exercici de les competències pròpies i alhora implementar un sistema de garanties reforçat per la legislació estatal de protecció de dades reformada.

En conseqüència, els apartats u i dos de l'article 3 RDL 14/2019, en el darrer incís dels nous articles 9.3 i 10.3 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, no vulneren les competències de la Generalitat *ex* article 159 EAC i troben empara en el títol competencial de l'article 149.1.18 CE, i s'adeqüen a les previsions dels articles 44 a 50 Reglament (UE) 2016/679.

C) Seguidament, farem referència a una altra de les mesures abans descrites, connectada amb l'anterior, continguda en sengles primers paràgrafs dels nous articles 9.3 i 10.3 LPACAP, que consisteix en l'obligatorietat que els recursos tècnics necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió dels sistemes d'identificació i signatura de les administracions públiques previstos als articles 9.2.*c* i 10.2.*c* LPACAP «estiguin situats en territori de la Unió Europea». I, en concret, quan es tracti de categories especials de dades previstes a l'article 9 del Reglament (UE) 2016/679, afegeixen que han de situar-se «en territori espanyol». Recordem que aquestes són les que revelin l'origen ètnic o racial, les opinions polítiques, les conviccions religioses o filosòfiques o l'afiliació sindical, i el tractament de dades genètiques, dades biomètriques dirigides a identificar de manera unívoca a una persona física, dades relatives a la salut o a la vida sexual o l'orientació sexual d'una persona física. En consonància amb aquesta obligació i per tal de garantir el seu compliment, les entitats del sector públic que gestionin directament o a través de mitjans propis els recursos tècnics necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió dels sistemes d'identificació i signatura han d'adoptar les mesures necessàries per ubicar els recursos emprats en territori europeu o, si escau, dins del territori espanyol, en el termini màxim de sis mesos a partir de l'entrada en vigor del Reial decret llei (disp. trans. primera, apt. 2).

Novament, el legislador estatal fonamenta aquesta doble restricció territorial en raons de seguretat pública i/o seguretat nacional i en la necessitat d'assegurar que l'Estat en el territori del qual s'ubiquin els recursos necessaris per gestionar els esmentats sistemes se sotmeti a la normativa de la Unió Europea en matèria de protecció de dades (apt. II, par. setè preàmbul RDL 14/2019). S'ha d'assenyalar, a tall d'indicació, que la mesura que ara es dictamina té com a complementària, en l'àmbit de la contractació pública, l'obligació que l'empresa adjudicatària informi, mitjançant la corresponent declaració, d'on estan ubicats els servidors i on es prestaran els

serveis associats a aquests, abans de la formalització del contracte (art. 122.2.*c* de la Llei 9/2017, de 8 de novembre, de contractes del sector públic, per la qual es traslladen a l'ordenament jurídic espanyol les directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014, segons la redacció donada per l'art. 5, apt. cinc, RDL 14/2019).

Ara bé, l'expressió «recursos tècnics necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió d'aquests sistemes» validats per les administracions públiques d'identificació electrònica dels administrats, anomenats de clau concertada i altres (art. 9.2.*c* LPACAP) i de signatura diferents als de signatura electrònica qualificada i avançada (art. 10.2.*c* LPACAP), sobre els quals es projecta la limitació territorial, té un abast genèric que, d'altra part, no està delimitat a la llei. Així, si acudim al Reglament (UE) 2016/679, defineix el «tractament» com a «qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunt de dades personals, ja sigui per procediments automatitzats o no, com la recollida, registre, organització, estructuració, conservació, adaptació o modificació, extracció, consulta, utilització, comunicació per transmissió, difusió, o qualsevol altra forma d'habilitació d'accés, confrontació o interconnexió, limitació, supressió o destrucció» (art. 4.2), cosa que ja inclou la «recollida» i l'«emmagatzematge» (citats expressament a la norma dictaminada). A aquest conjunt d'activitats el Reial decret llei afegeix la de «gestió dels sistemes», que no s'acaba de copsar quin abast pot tenir. En definitiva, som davant d'una restricció que, en principi, afectaria principalment la ubicació dels servidors i els serveis associats, però que podria incloure també altres recursos i elements associats a aquells.

D'aquesta manera, hom pot albirar que el Reial decret llei pretén exercir un control de les dades, entre d'altres situacions i possibilitats, davant la nova forma de prestació dels serveis de tractament de la informació, anomenada *cloud computing* o computació en el núvol. De forma resumida, ja que és una

qüestió complexa tècnicament, en un entorn de *cloud computing* la gestió de la informació és de forma virtual en poder del client (que pot ser una administració pública), que la tracta a través d'internet tot accedint a solucions de bases de dades, correu electrònic o qualsevol tipus d'aplicacions segons les seves necessitats, mentre que el proveïdor del servei pot trobar-se, pràcticament, en qualsevol lloc del món i proporcionar els serveis mitjançant pràctiques de deslocalització, compartició de recursos i mobilitat o realitzant subcontractacions addicionals. Així, la multiubiqüitat de les dades en el núvol s'articula sovint mitjançant una cadena de subcontractacions que, comporten, en molts casos (tot i que no ha de ser així necessàriament) transferències internacionals.

Aquesta forma d'emprar tecnologies de la informació i la comunicació que ja existien a una nova escala la fa diferent, ja que permet l'ús de recursos de maquinari, programari, emmagatzematge, serveis i comunicacions que es troben distribuïts geogràficament i als quals s'accedeix de forma dinàmica mitjançant una xarxa (gratuïta o abonant una tarifa) i proporciona als seus clients un servei de tecnologies de la informació sota demanda i de gran flexibilitat. Com a conseqüència d'això, el client (o contractista) pot desconèixer la localització precisa de les dades que tracta i no disposar del control directe i d'accés a aquestes, ni de la seva eliminació i portabilitat, ja que la informació no està físicament en el seu poder, per bé que, si conté dades personals, sí que és el responsable d'aquestes des del punt de vista del Reglament (UE) 2016/679.

En aquest entorn, doncs, intervenen diversos subjectes: l'usuari o client (pot ser una administració pública) que contracta i utilitza els serveis de *cloud computing* o recursos informàtics a través de la xarxa, i el proveïdor, que és un tercer que proporciona aquests serveis en el núvol. A part de clients i proveïdors, poden concórrer-hi també altres subjectes (subcontractats), com és el cas dels socis o *partners* del proveïdor de *cloud*, que ofereixen i

suporten serveis addicionals de valor afegit. En funció de com sigui aquest valor afegit, es pot parlar de diferents modalitats de contractació per part del client o usuari final: una solució d'infraestructura com a servei o IaSS (capacitat d'emmagatzematge i procés en brut a través de la xarxa i servidors d'allotjament web) quan el valor afegit és nul perquè l'usuari final ha de construir les aplicacions que necessita pràcticament des de zero; una solució de plataforma com a servei o PaSS, mitjançant la qual es proporcionen utilitats per construir aplicacions i desenvolupar solucions (bases de dades o entorns de programació, entre d'altres), o una solució de programari com a servei o SaaS, quan l'usuari troba al núvol eines finals amb les quals pot implementar directament els processos que li interessen (una aplicació de comptabilitat, de correu electrònic, un programa de gestió documental, etc.).

Per tant, atès que les dades poden estar en qualsevol moment en qualsevol lloc (*data can be collected in Germany, stored in India and processed in the Unites States*), però els drets i les obligacions relatius a aquestes s'han de garantir en tot cas, el RDL 14/2019 conté diversos mecanismes per evitar aquestes situacions d'incertesa i garantir així la protecció de les dades personals, com poden ser la verificació pel contractista de les condicions en què el proveïdor ha de prestar el servei, incloent-hi la sol·licitud d'informació sobre la ubicació del tractament, sobre l'existència de subcontractació i les polítiques de seguretat que segueix, sobre els drets dels usuaris i les obligacions legals que es compromet a observar. Altres instruments també poden facilitar aquest control, com és el cas de l'aplicació per part del proveïdor de la norma ISO/IEC 27018, de 29 de juliol de 2014, sobre els requisits per a la protecció de la informació d'identificació personal (PII) en sistemes *cloud*, de conformitat amb els principis de privacitat en la norma ISO/IEC 29100, per a entorns de treball amb sistemes d'emmagatzematge en el núvol.

Tot i així, l'aplicació de les cauteles previstes no sempre és fàcil, tant per les peculiaritats que s'han descrit (el caràcter dinàmic i canviant de la ubicació física de les dades) com perquè hi pot haver manca de transparència per part del proveïdor o un insuficient control per part del responsable (contractista). En aquest sentit, atès que les regles i els controls en matèria de transferències internacionals de dades personals, tot i ser efectives, poden no ser suficients quan es tracta de la prestació de serveis *cloud*, s'ha considerat que una part de la solució podria ser el desenvolupament de l'*European cloud computing centres or EU-based clouds* per assegurar als clients que les dades personals es tractaran en el si de la Unió Europea o en països amb garanties adequades («*The reform of the EU Data Protection Directive: the impact on business European Business Summit Brussels*» SPEECH/11/349 de la Comissaria de Justícia de la Comissió Europea, de 18 de maig de 2011, i, en aquest sentit, la iniciativa de la Comissió Europea *The European Cloud Strategy 2012*).

En aquest panorama, la limitació aprovada pel Reial decret llei evitaria ja d'entrada la deslocalització dels recursos fora de la Unió Europea de tots els subjectes que intervenen, de forma directa o subcontractada, en la provisió dels serveis i la gestió dels sistemes d'informació objecte de la mesura. Per tant, resulta clar que el legislador estatal ha anat més enllà del Reglament (UE) 2016/679 i ha aprovat una limitació que, *per se*, ja facilita d'entrada el control dels tractaments de les dades personals afectades pels sistemes d'identificació i signatura electròniques que preveuen els articles 9.2.*c* i 10.2.*c* LPACAP, que afavoreix el compliment del nivell de protecció adequat atorgat per les normes europees i estatals en la seva totalitat.

I això fins al punt que difícilment podran tenir lloc transferències internacionals de dades en la gestió d'aquests sistemes si tots els recursos tècnics necessaris per a la prestació del servei han d'estar localitzats en el territori europeu. En altres paraules, la prohibició general de deslocalització

de les instal·lacions és una mesura més restrictiva que la regla aplicable a les transferències internacionals de categories especials de dades que es recull a continuació i que hem examinat anteriorment, ja que és una restricció addicional que no permet ubicar sistemes en *cloud* de tercers països o organitzacions internacionals, fins i tot en els casos en què aquests gaudeixin d'una decisió d'adequació o es tracti de complir amb una obligació internacional.

Ara bé, deixant de banda la defectuosa tècnica legislativa emprada, i per les mateixes raons que hem sostingut en l'examen de la limitació de les transferències internacionals, hom pot dir que la limitació de localitzar els recursos necessaris, en la mesura que comprèn la totalitat del territori de la Unió Europea, és legítima des del punt de vista del dret fonamental de l'article 18.4 CE i no és contrària al Reglament (UE) 2016/679. Igualment, ha estat dictada pel legislador sectorial estatal en desenvolupament de les garanties de l'administrat i a l'empara de les competències previstes a l'article 149.1.18 CE.

No podem arribar a la mateixa conclusió respecte a l'obligació de situar els recursos tècnics únicament «en territori espanyol» que, a parer nostre, vulneraria els principis i les previsions del citat Reglament (UE) 2016/679 perquè constituiria una mesura innecessària i desproporcionada, per molt que es tracti de protegir les categories especials de dades. Així, d'aquesta mesura legal estatal en resulta que els tractaments de dades fóra d'Espanya restarien prohibits, equiparant-se el seu règim jurídic més al d'una transferència internacional que no pas al que correspon a l'espai europeu. Recordem que, precisament, amb l'aplicació del Reglament europeu s'assoleix un nivell uniforme i elevat de protecció dels drets i les llibertats de les persones físiques pel que fa al tractament de les seves dades personals que permet eliminar els obstacles a la circulació de dades personals en el seu territori.

I, per tant, és innecessària perquè el conjunt d'estats de la Unió Europea que constitueixen l'àmbit d'aplicació territorial del Reglament (UE) 2016/679 estan sotmesos a prescripcions i garanties equivalents, com resulta evident i immediat del fet de formar part del mateix ordenament jurídic i, consegüentment, cap motiu sembla que podria avalar una mesura que pressuposa una insuficient cobertura, o la necessitat d'una major protecció, respecte de la resta d'estats membres que formen part de la Unió Europea. En el cas d'Espanya, cal recordar que de l'article 93 CE es deriva que l'ordenament estatal integra com a dret propi el dret europeu en una posició jeràrquica immediatament inferior a la Constitució i els tractats internacionals, i del qual en són font superior els reglaments comunitaris.

I, a més d'innecessària, afegim que és una norma desproporcionada atès que el resultat de la seva presumpta adopció podria afectar el principi de llibertat d'establiment garantit en els tractats originaris de la Unió Europea. I això seria així perquè, tal com també ho hem indicat, aquesta regla limitaria de manera no raonable la lliure competència entre operadors econòmics o empreses a l'hora de competir en el conjunt de l'EEE, en la mesura que els fixaria una condició obstructiva i desmesurada de restricció de la ubicació dels seus recursos —circumscrita al territori espanyol— que els restaria llibertat i incidiria en el principi de competència en igualtat de condicions.

En conclusió, els apartats u i dos de l'article 3 RDL 14/2019, de 31 d'octubre, en l'obligació que incorporen als articles 9.3 i 10.3 LPACAP de situar els recursos tècnics necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió dels sistemes dels articles 9.2.*c* i 10.2.*c* LPACAP «en territori espanyol», com també la disposició transitòria primera, apartat 2 RDL 14/2019, quan regula el règim transitori de la dita obligació, són contraris als principis del Reglament (UE) 2016/679, pel que fa a la lliure circulació de dades personals en el mercat interior (art. 1 i considerant 13).

Dit això, creiem oportú recordar al Govern que la contradicció d'un reglament europeu no es pot dirimir, en sentit estricte, en el si de la jurisdicció constitucional, en tractar-se d'un supòsit de legalitat ordinària i selecció del dret aplicable, del qual en té la darrera paraula el Tribunal de Justícia de la Unió Europea.

D) L'apartat u de l'article 4 RDL 14/2019 introdueix un nou article 46 bis a la LRJSP, el text del qual diu el següent:

> «Els sistemes d'informació i comunicacions per a la recollida, l'emmagatzematge, el processament i la gestió del cens electoral, els padrons municipals d'habitants i altres registres de població, dades fiscals relacionades amb tributs propis o cedits i dades dels usuaris del sistema nacional de salut, així com els corresponents tractaments de dades personals, s'han d'ubicar i prestar dins del territori de la Unió Europea. Les dades a què es refereix l'apartat anterior no poden ser objecte de transferència a un tercer país o organització internacional, a excepció dels que hagin estat objecte d'una decisió d'adequació de la Comissió Europea o quan així ho exigeixi el compliment de les obligacions internacionals assumides pel Regne d'Espanya.»

Com es pot constatar, aquest precepte, atesos el seu contingut i la seva finalitat, conté un seguit de mesures equiparables a les examinades en els apartats anteriors, si bé en aquest cas projectades sobre la Llei del règim jurídic del sector públic i altres sistemes d'informació i comunicació que gestionen habitualment les administracions públiques. En concret, els relatius als padrons municipals d'habitants i altres registres de població, els de dades fiscals relacionades amb tributs propis o cedits i els de dades dels usuaris del sistema nacional de salut. Això és: d'una banda, s'estableix la regla general que no es poden efectuar transferències internacionals de les dades personals que tracten llevat que es facin a tercers països que hagin estat

objecte d'una decisió d'adequació de la Comissió o que siguin resultat del compliment d'una obligació internacional assumida per Espanya.

I, de l'altra, s'incorpora també la limitació de la localització dels recursos «dins del territori de la Unió Europea», que es tradueix novament en l'obligació que els dits sistemes d'informació i comunicacions, així com els corresponents tractaments de dades personals, s'han d'ubicar i prestar dins del territori europeu. En aquest darrer cas, sembla que es distingeix entre instal·lacions físiques i tractaments, cosa que no és esclaridora, i aplica les mateixes mesures a les dades relatives a la salut que, com se sap, són dades especials, a altres dades que no ho són però que, per la naturalesa de la informació que afecten, el legislador estatal ha considerat que es poden sotmetre a unes condicions o limitacions específiques, tenint en compte que també s'ha d'observar allò que estableixi la normativa sectorial que els resulta aplicable.

Segons això, les entitats del sector públic han d'adoptar les mesures necessàries per ubicar, o reubicar, en territori europeu, els recursos que utilitzin per gestionar directament o a través de mitjans propis els sistemes d'informació i comunicacions a què es refereix l'article 46 bis, en el termini de sis mesos a partir de l'entrada en vigor del Reial decret llei (6 de maig de 2020) (disp. trans. segona, apt. 1).

Cal destacar que la principal diferència amb els articles examinats en els apartats anteriors és que el nou article 46 bis LRJSP no preveu la restricció més intensa de la ubicació dels recursos en el territori espanyol sinó que, com hem dit, exigeix que estiguin localitzats dins de la Unió Europea.

I l'anterior malgrat que aquesta norma també comprèn dades relatives a la salut (en aquest cas del Sistema Nacional de Salut), que hem vist que sí que estan sotmeses a l'esmentada obligació de localització en territori espanyol

quan són objecte de tractament per determinats sistemes d'identificació i signatura gestionats per les administracions públiques. Altrament, el preàmbul, referint-se a aquest concret article, justifica també la restricció territorial que s'hi conté «per raons de seguretat pública», sense ulteriors explicacions. I, quan es refereix a la regla sobre la transferència internacional de dades, parla erròniament de cessió de dades.

Però, al marge d'aquestes observacions crítiques, es poden aplicar al nou article 46 bis LRJSP les mateixes consideracions efectuades respecte a la regla general de limitació de les transferències internacionals, admeses només en casos de decisió d'adequació o de compliment d'una obligació internacional assumida per Espanya, i a l'exigència de situar els recursos en territori europeu. En conseqüència, l'apartat u de l'article 4 RDL 14/2019 i la disposició transitòria segona del RDL 14/2019 no vulneren les competències de la Generalitat sobre règim de les administracions públiques *ex* article 159 EAC i troben empara en el títol competencial de l'article 149.1.18 CE.

E) L'apartat dos de l'article 4 RDL 14/2019 dona una nova redacció a l'article 155 LRJSP, que diu que:

> «1. De conformitat amb el que disposen 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 dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE, i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, i la seva normativa de desplegament, cada Administració ha de facilitar l'accés de la resta d'administracions públiques a les dades relatives als interessats que tingui en el seu poder, i ha d'especificar les condicions, els protocols i els criteris funcionals o tècnics necessaris per accedir a aquestes dades amb les màximes garanties de seguretat, integritat i disponibilitat.

> 2. En cap cas es pot procedir a un tractament ulterior de les dades per a finalitats incompatibles amb la finalitat per a la qual es van recollir inicialment les dades personals. D'acord amb el que preveu l'article 5.1.b) del Reglament (UE) 2016/679, no es considera incompatible amb les finalitats inicials el tractament ulterior de les dades personals amb finalitats d'arxiu en interès públic, finalitats de recerca científica i històrica o finalitats estadístiques.
>
> 3. Fora del cas que preveu l'apartat anterior i sempre que les lleis especials aplicables als tractaments respectius no prohibeixin expressament el tractament ulterior de les dades per a una finalitat diferent, quan l'Administració pública cessionària de les dades pretengui el tractament ulterior d'aquestes per a una finalitat que consideri compatible amb la finalitat inicial ho ha de comunicar prèviament a l'Administració pública cedent a l'efecte que aquesta pugui comprovar la compatibilitat. L'Administració pública cedent s'hi pot oposar motivadament en el termini de deu dies. Quan l'Administració cedent sigui l'Administració General de l'Estat pot suspendre en aquest supòsit, excepcionalment i de manera motivada, la transmissió de dades per raons de seguretat nacional de manera cautelar pel temps estrictament indispensable per a la seva preservació. Mentre l'Administració pública cedent no comuniqui la seva decisió a la cessionària aquesta no pot utilitzar les dades per a la nova finalitat pretesa. S'exceptuen del que disposa el paràgraf anterior els supòsits en què el tractament per a una altra finalitat diferent d'aquella per a la qual es van recollir les dades personals estigui previst en una norma amb rang de llei de conformitat amb el que preveu l'article 23.1 del Reglament (UE) 2016/679.»

Amb relació a aquest precepte, el sol·licitant al·lega que el règim jurídic de caràcter general per a les comunicacions de dades entre administracions públiques comportaria una restricció desproporcionada de les competències reconegudes a la Generalitat en matèria d'organització de la seva Administració i sobre règim jurídic i procediment administratiu, en els termes previstos en els articles 150 i 159 EAC.

Per la seva part, el preàmbul del Reial decret llei argumenta que l'objectiu de la reforma «és permetre un control més gran de les dades cedides entre administracions públiques, a l'efecte de garantir-ne la utilització adequada», situant el precepte analitzat en el context del Reglament (UE) 2016/679 quant a la regulació que efectua de la licitud del tractament de les dades personals per a finalitats diferents de les inicialment previstes (apt. II, par. dotzè i tretzè). I la disposició final primera, apartat 2, declara que aquest precepte ha estat dictat a l'empara dels articles 149.1.18 i .29 CE.

En aquest sentit, centrant-nos en l'àmbit sobre el qual incideix l'article 155 LRJSP, ara modificat, cal recordar, molt sintèticament, que segons la norma europea, les dades que s'han recollit per a finalitats determinades, explícites i legítimes, no es poden tractar amb posterioritat de manera incompatible amb aquestes finalitats. En relació amb això, el Reglament (UE) 2016/679 estableix la presumpció general que són en tot cas activitats compatibles amb una altra d'anterior els tractaments que tinguin finalitats d'arxiu en interès públic, d'investigació científica i històrica o estadístiques, per bé que estan igualment sotmesos al compliment d'un seguit de garanties adequades, com poden ser el principi de minimització, anonimització o pseudonimització (art. 5.1.*b* i 89.1 RGPD). Per tal de determinar si el tractament posterior amb distinta finalitat és o no compatible amb la finalitat per la qual es van recollir inicialment les dades personals, l'esmentada norma europea dona alguns elements o criteris de valoració: entre altres coses, s'ha de tenir en compte el context en què es van recollir aquestes dades o les expectatives raonables de l'interessat basades en la seva relació amb el responsable quant al posterior ús de les seves dades (art. 6.4 RGPD i considerant 50). En cas que l'interessat hagi estat informat i hagi donat el seu consentiment explícit, aquesta comprovació no resulta necessària.

Dit això, els dos primers apartats de l'article 155 LRJSP, segons la redacció donada pel Reial decret llei, traslladen aquesta regulació europea a l'àmbit de

les comunicacions o transmissions de dades entre administracions públiques per a l'exercici de les seves funcions, que presenta peculiaritats pròpies. I ho fan remetent-se al Reglament europeu, reproduint-ne parcialment les seves previsions (tècnica legislativa que admet el considerant 8 RGPD als efectes d'una millor comprensió de la norma interna) i, complementàriament, establint l'obligació que cada Administració ha de facilitar l'accés de la resta d'administracions públiques a les dades relatives als interessats que tingui en el seu poder per bé que mitjançant un procediment que asseguri les màximes garanties de seguretat, integritat i disponibilitat.

Pel que fa a l'apartat 3, regula el procediment o tràmit interadministratiu que permeti valorar i comprovar si la finalitat ulterior a la qual es vol destinar les dades és o no compatible amb la que inicialment va legitimar el seu tractament, establint una obligació addicional de consulta a l'Administració que comunica les dades. D'aquesta manera, l'Administració destinatària de les dades, responsable del nou tractament, no el podrà dur a terme (per molt que el consideri compatible) fins que, prèviament, ho hagi comunicat a l'Administració que les va recollir inicialment, la qual pot comprovar que, efectivament, es dona l'esmentada compatibilitat i, en cas contrari, pot oposar-s'hi en un termini de deu dies. Per a aquesta comprovació, tindrà en compte els criteris establerts a l'article 6.4 RGPD, a què hem fet esment abans.

Seguidament, el mencionat apartat 3, en aplicació de les previsions de l'article 23.1 RGPD (i del mateix art. 6.4), disposa que aquesta garantia o procediment interadministratiu de constatació de la finalitat compatible pot ser exceptuat quan una norma amb rang de llei estableixi que el tractament per a una finalitat diferent es fonamenta en una «mesura necessària i proporcional en una societat democràtica». Així, segons la remissió que s'hi conté: per salvaguardar la seguretat de l'Estat, la defensa, la seguretat pública, la prevenció, la investigació, la detecció o l'enjudiciament

d'infraccions penals o l'execució de sancions penals, els objectius d'interès econòmic o financer importants (incloent-hi els àmbits fiscals, pressupostari, monetari, de sanitat pública i la seguretat social), l'exercici de l'autoritat pública, la protecció de la independència judicial, de l'interessat i dels drets i llibertats dels altres o l'execució de demandes civils.

De fet, la mateixa norma objecte de dictamen incorpora una excepció a la regulació procedimental que s'hi preveu, quan declara que l'Administració general de l'Estat pot suspendre la transmissió de les dades personals per «raons de seguretat nacional», si bé exigeix que la dita potestat de suspensió tingui caràcter excepcional i cautelar i s'adopti de manera motivada i pel temps estrictament indispensable per a la preservació de l'esmentada seguretat.

Fins aquí ens trobem davant d'una regulació que es remet a la normativa europea respecte als principis i les condicions generals per a un tractament lícit de les dades i la transcriu parcialment, alhora que desenvolupa altres aspectes concrets del dret fonamental *ex* article 18.4 CE quan es projecta sobre el sector públic. No som, per tant, davant la regulació del contingut essencial de l'esmentat dret fonamental sinó d'una norma sectorial dictada pel legislador estatal a l'empara de l'article 149.1.18 CE, que determina les especificitats i les garanties adequades per preservar els drets i les llibertats de les persones titulars de les dades quan aquestes són objecte de comunicació o transmissió entre les administracions públiques, ja sigui amb l'objectiu de facilitar l'exercici de les funcions i les competències pròpies d'aquestes, ja sigui per fer efectius altres drets dels administrats en aquest concret àmbit material, com és el cas de l'article 28.2 LPACAP. Recordem que aquest precepte atorga als interessats el dret a no aportar en un procediment administratiu els documents que ja es trobin en poder de l'Administració davant la qual actua o que hagin estat elaborats per qualsevol altra Administració pública.

Val a dir que el mateix precepte preveu com a mesura restrictiva la suspensió de la transmissió de les dades entre les administracions implicades quan es tracti de preservar altres objectius d'interès públic, en concret, la protecció de la seguretat nacional (art. 149.1.29 CE). En aquest cas, entenem que la seguretat nacional constitueix un pressupòsit habilitant qualificat que pot operar com a excepció del règim general de comunicació de dades entre administracions públiques. Així, considerem que aquest concepte, segons la jurisprudència constitucional recent (STC 184/2016, de 3 de novembre, FJ 3 i 4, i en el mateix sentit els DCGE 18/2015, FJ 3 i 4; 5/2017, FJ 2 i 3), esdevé una submatèria amb unes notes de risc estructural, sistèmic i global que superen la noció de la seguretat pública en un sentit ordinari, vinculada a la protecció de persones i béns. En el cas de la seguretat nacional, la potencial amenaça es connecta amb la matèria de defensa (art. 149.1.4 CE), concurrència aquesta que ens remet a situacions de crisi que podrien consistir en riscos excepcionals d'atemptats terroristes o ciberatacs a escala internacional, per esmentar alguns exemples prou reveladors. I aquesta esfera, com resulta evident, recau de manera clara i immediata en l'àmbit de la competència exclusiva de l'Estat, en coordinació i cooperació, en el cas de Catalunya, com també és evident, amb les autoritats autonòmiques catalanes i el cos de Mossos d'Esquadra.

D'altra banda, la mateixa norma incorpora un seguit de cauteles o garanties per delimitar aquesta potestat estatal de suspensió, que defineix com excepcional: tindrà caràcter cautelar i s'adoptarà de forma motivada i pel temps estrictament indispensable per a la seva preservació.

Per tot el que s'ha exposat, entenem, doncs, com en els supòsits examinats en apartats anteriors, que la norma no vulnera les competències de l'Administració de la Generalitat respecte del procediment i el règim jurídic de les administracions públiques previstes a l'article 159.2 EAC.

En conclusió, l'apartat dos de l'article 4 del Reial decret 14/2019, que dona nova redacció a l'article 155 LRJSP, s'adequa al Reglament (UE) 2016/679 i no vulnera les competències de la Generalitat respecte del règim jurídic de les administracions públiques *ex* article 159.1 i .2 EAC, atès que troba empara en els títols competencials de l'article 149.1.18 i .29 CE.

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

C O N C L U S I O N S

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 i, en concret, els articles 1, 2, 3, 4, 6, 7, les disposicions addicional única i transitòries primera i segona i la disposició final primera, són contraris a l'article 86.1 CE, perquè no compleixen 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 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.
Adoptada per unanimitat.

Quarta. L'article 6.cinc del Reial decret llei 14/2019, en la redacció que dona a l'apartat 1 de l'article 81 de la Llei 9/2014, és inconstitucional perquè vulnera l'article 9.3 CE, ja que no compleix les exigències de qualitat normativa, tant pel que fa a la incorporació de les garanties dels ciutadans com a la previsibilitat de la seva aplicació.
Adoptada per unanimitat.

Cinquena. 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.

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.