Nota en relació amb el Dictamen del Consell de Garanties Estatutàries 1/2020, de 23 de gener, sobre el Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions

Com a qüestió prèvia, cal assenyalar que el Consell s'ha pronunciat sobre aquesta mateixa norma legal en el Dictamen 6/2019, de 30 de desembre, emès a petició del Govern de la Generalitat, la qual va examinar des de la perspectiva de la seva adequació constitucional a l'article 86.1 CE alhora que va efectuar l'escrutini de constitucionalitat i d'estatutarietat dels preceptes següents del Reial decret llei 14/2019: articles 1; 2; 3.u i .dos; 4; 6.u, .dos i .cinc, i 7; la disposició addicional única, i, per connexió, les disposicions transitòries primera, apartats 1 i 2; segona, i la disposició final primera. El present Dictamen, doncs, parteix d'aquesta opinió consultiva precedent i emet el seu parer, a més, respecte de l'article 3.tres, en la nova disposició addicional sisena que afegeix a la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.

Conclusions del Dictamen:

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

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

En el fonament jurídic 2.1 del DCGE 6/2019 s'ha fet referència expressa a la inexistència d'una acreditació explícita i raonada, que pogués justificar el compliment de l'extraordinària i urgent necessitat, descartant la virtualitat de les clàusules rituals i abstractes de l'argumentació del Govern estatal en el preàmbul de la norma.

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.

L'article 3.u i .dos RDL 14/2019 modifica, entre d'altres, la lletra *c* dels articles 9.2 i 10.2 Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques (en endavant, LPACAP), que accepten l'ús dels sistemes d'identificació i de signatura electrònica de clau concertada o d'altres que comptin amb un registre previ com a usuari que permeti garantir-ne la identitat i que les administracions considerin vàlid si bé, com a novetat, aquesta categoria de sistemes d'identificació i signatura electrònica se sotmet a un règim

d'autorització prèvia per part 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. El termini màxim d'emissió de l'autorització és de tres mesos i la manca de resolució dins de l'esmentat termini té efectes desestimatoris. La qüestió debatuda respecte els articles 9.2.*c* i 10.2.*c* LPACAP se centra en l'esmentada autorització prèvia atribuïda a l'Administració general de l'Estat en termes idèntics en ambdós preceptes.

Per tal de procedir a l'enquadrament competencial dels preceptes examinats, primerament cal acudir a la disposició final primera RDL 14/2019, relativa als títols competencials corresponents a cada article. Concretament, l'article 3 RDL 14/2019 es dicta segons aquesta disposició 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).

La rúbrica general del RDL 14/2019 corrobora la 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 interessa, és el relatiu a l'administració digital (art. 149.1.18 CE). Així mateix, les referències generals del preàmbul incideixen en els dos títols mencionats.

Més concretament, el preàmbul del Reial decret llei situa el contingut dels articles 3 i 4 RDL 14/2019 en relació amb les administracions públiques (apt. II, par. tercer), tot i que especifica 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).

Ara bé, a l'hora d'escatir el títol competencial prevalent, es descarta la competència en seguretat pública perquè hi ha un ús excessivament expansiu en la seva utilització sobre l'objecte del Reial decret llei. En aquest sentit, el Tribunal Constitucional 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).

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, de 29 de juny, 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 dins de les bases estatals.

Donat el contingut dels diferents aspectes que configuren el concepte de ciberseguretat, s'entén que pot tenir diferents accepcions i estendre's a diverses activitats (STC 142/2018, de 20 de desembre, 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).

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). 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).

Els preceptes examinats del Reial decret llei contenen 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, s'enquadra prevalentment dins l'article 149.1.18 CE, tot i que hi pot incidir excepcionalment el títol de seguretat pública de l'article 149.1.29 CE.

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.

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), si bé 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).

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 (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, 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). 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, entre d'altres, les quals poden ser ampliades segons les circumstàncies del cas concret.

Per la seva banda, 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» (DCGE 23/2015, de 17 de desembre, 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), sense que l'Estat pugui interferir en l'organització interna de les comunitats autònomes.

En el supòsit examinat, 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, 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 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* estableixen l'obligació que els usuaris estiguin registrats prèviament per garantir-ne la identitat.

Per tant, 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.

La previsió qüestionada constitueix més aviat una tutela o un control sobre l'administració autonòmica, de caràcter previ, fet que, amb independència del sentit de l'autorització estatal, condiciona el procediment administratiu autonòmic de resolució.

En aquest sentit, els informes previs preceptius i vinculants per part de l'Estat, com a mitjà d'integració de dues competències concurrents de titularitat autonòmica i estatal, només són legítims si se suporten en una competència estatal, quan efectivament es doni la projecció d'aquesta i es resolguin basant-se en ella (STC 18/2011, de 3 de març, F 21.*a*, i DCGE 7/2014, de 27 de febrer, FJ 3.3). A més a més, 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*).

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.

En conclusió, les previsions d'autorització prèvia de l'article 9.2.*c* i 10.2.*c* LPACAP no constitueixen un control emparat per les bases estatals ni per l'establiment d'un procediment comú, i interfereixen en la competència de la Generalitat de permetre autoritzar sistemes, fins a poder-l'hi impedir, sense que l'Administració general de l'Estat disposi de competències sobre l'autorització dels sistemes d'identificació dels interessats davant l'Administració catalana.

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.

Tercera. *L'article 3.u i .dos del Reial decret llei 14/2019, en l'obligació que incorpora als articles 9.3 i 10.3 de la Llei 39/2015 de situar «en territori espanyol» els recursos tècnics necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió dels sistemes previstos en els articles 9.2.c i 10.2.c de l'esmentada Llei, com també, per connexió, la disposició transitòria primera, apartat 2, del mateix Reial decret llei, són contraris al principi de lliure circulació de dades previst a l'article 1 del Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27*

d'abril de 2016, relatiu a la protecció de les persones físiques, quant al tractament de dades personals i a la lliure circulació d'aquestes i pel qual es deroga la Directiva 95/46/CE.
Adoptada per unanimitat.

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, RGPD] 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. Des d'una perspectiva formal, el Reglament és 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.

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 recorda 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 citació de la STC 140/2018, de 20 de desembre, FJ 6).

El dret fonamental a la protecció de dades, 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. 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).

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.

Pel que fa a la transferència internacional de dades, es tracta d'un concepte complex, 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 un trasllat físic i efectiu d'aquestes per part d'una persona física o jurídica, pública o privada, o d'un òrgan o entitat administratius situats en territori espanyol a un altre d'un país tercer o a una organització internacional que es troben fora de l'espai de nivell adequat o equiparable de protecció, en aquest cas 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). I això anterior, amb la finalitat última de tractar aquesta informació un cop hagi estat rebuda pel destinatari.

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). Vist aquest principi general, el Reglament (UE) 2016/679 permet la transferència internacional de dades només en alguns supòsits taxats, com ara l'existència d'una decisió d'adequació de la Comissió Europea o la de garanties adequades i que l'interessat compti amb drets exigibles i accions legals efectives, dels quals cal informar-lo (art. 45 i 46), si bé a continuació l'admet en un ventall d'excepcions per a situacions específiques, en llista tancada o *numerus clausus (*art. 49).

Els primers paràgrafs dels nous articles 9.3 i 10.3 LPACAP estableixen l'obligatorietat que els recursos tècnics necessaris per a la recollida, l'emmagatzematge, el tractament i la gestió dels 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) «estiguin situats en territori de la Unió Europea». I, en concret, quan es tracti de categories especials de dades previstes a l'article 9 Reglament (UE) 2016/679, afegeixen que han de situar-se «en territori espanyol». Cal recordar 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. I que, atesa la seva naturalesa, són particularment sensibles i, conseqüentment, 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).

Les entitats del sector públic que gestionin directament o a través de mitjans propis els dits recursos tècnics disposen d'un termini màxim de sis mesos a partir de l'entrada en vigor del

Reial decret llei per adoptar les mesures necessàries per ubicar-los en territori europeu o, si escau, dins del territori espanyol (disp. trans. primera, apt. 2).

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, sobre els quals es projecta la limitació territorial, té un abast genèric que, d'altra part, no està delimitat a la llei, i 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.

En la mesura que la restricció examinada es regula juntament amb altres limitacions relatives a la transferència internacional de dades, es pot albirar que el Reial decret llei pretén exercir un control d'aquestes, 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 panorama, en el que les dades personals poden estar en qualsevol moment en qualsevol lloc, 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 electrònica 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, 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, la limitació de localitzar els recursos necessaris, en la mesura que comprèn la totalitat del territori de la Unió Europea, és una mesura protectora i 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 es pot arribar a la mateixa conclusió respecte a l'obligació de situar els recursos tècnics únicament «en territori espanyol», la qual 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. Cal tenir present 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 sembla, doncs, que cap motiu 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, 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 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, resulta 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 té la darrera paraula el Tribunal de Justícia de la Unió Europea.

Quarta. *L'article 3.tres del Reial decret llei 14/2019, en la nova disposició addicional sisena que afegeix a la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, vulnera les competències de la Generalitat ex article 159 EAC i no*

troba empara en l'article 149.1.18 i .29 CE. Per connexió, la disposició final primera, apartat 2, del Reial decret llei 14/2019 també les vulnera i tampoc no troba empara en els preceptes constitucionals citats.
Adoptada per unanimitat.

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

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

D'acord amb l'article 149.1.18 CE, l'Estat pot establir bases en l'àmbit descrit (la disciplina sobre la identificació i signatura electrònica dels interessats en les seves relacions amb les administracions públiques) sempre que preservin els marges d'autoorganització de les administracions públiques autonòmiques i les seves competències en aquesta matèria. Això és, que aquestes administracions han de poder adoptar les decisions relatives al model d'organització i funcionament de la seva administració electrònica i de les relacions digitals que mantenen amb els ciutadans i, per tant, dels sistemes d'identificació i de signatura electròniques i de la tecnologia en la qual es basaran que considerin que s'ajusta més a les seves necessitats. Així ho ha reconegut expressament el Tribunal Constitucional, quan ha declarat que les polítiques autonòmiques en l'àmbit de la identificació electrònica (art. 9 LPACAP, versió anterior a la reforma pel RDL 14/2019) poden ser molt diverses i han de preservar amplis marges d'autoorganització de les administracions públiques en aquest entorn. Per tant, les comunitats autònomes poden optar per emprar sistemes que puguin tenir virtualitat en altres estats membres de la Unió Europea, o bé poden ser proclius a utilitzar instruments senzills de baix nivell de seguretat per a ús domèstic (STC 55/2018, de 24 de maig, FJ 9).

Amb tot, la regulació governamental pretesament bàsica que és objecte del Dictamen no respecta aquesta darrera observació de caràcter competencial. Es tracta d'una mesura de naturalesa singular que proscriu de manera preventiva i posposa indefinidament l'ús d'una determinada tecnologia per part de les administracions públiques, tot posposant la seva futura admissió a l'eventual compliment d'una condició indefinida en el temps, la realització de la qual depèn, de fet, de l'Estat mateix. I adopta aquesta solució tan expeditiva en comptes d'establir, com li pertocaria competencialment, els principis o criteris que les administracions públiques haurien de respectar, en relació amb aquesta tecnologia, i que constituirien unes bases més estandarditzades, a l'empara de la matèria reservada a l'Estat per l'article 149.1.18 CE.

A més, s'aparta de la voluntat neutral i més aperturista del Reglament eIDAS (considerants 16 i 26) i de les resolucions aprovades pel Parlament Europeu en aquest sector. Altrament, tampoc no s'albira què succeiria si, en aplicació d'aquella norma europea i el seu principi de reconeixement mutu (art. 6), l'Estat espanyol admet la validesa de sistemes d'identificació i de signatura electròniques d'altres estats membres basats, precisament, en la tecnologia de registre distribuït.

En el cas que s'analitza no es tracta d'una prohibició en el sentit de mera limitació que ha d'observar la Generalitat a l'hora de regular i executar una matèria. Al contrari, més enllà del que seria una base pròpiament dita, mitjançant la prohibició d'una específica tecnologia, l'Estat

deixa sense efecte l'exercici d'una competència que correspon a les comunitats autònomes perquè està desnaturalitzant i pràcticament impedint la possibilitat d'establir una política pròpia en el sector afectat. I això és així perquè, per definició, adoptar una política concreta en un determinat entorn comporta la capacitat de la Generalitat de triar lliurement entre les diverses possibilitats, en funció de les que li resultin més adequades o idònies segons les seves necessitats. Pel que ara interessa, respecte al disseny i la configuració pròpia dels instruments administratius d'identificació i de signatura electrònica en les relacions digitals dels ciutadans amb l'Administració pública catalana.

Es tracta d'una previsió si més no peculiar que, pel seu caràcter fortament restrictiu, merita una explicació fonamentada i raonada que en justifiqui l'adopció, en la mesura que l'Estat s'arroga una potestat de la Generalitat (com és el disseny dels sistemes d'identificació i de signatura dels interessats en les seves relacions amb l'Administració catalana) que troba empara en l'article 159 EAC. Dit això, en la nova disposició addicional sisena.1 LPACAP no hi ha cap justificació de la regla prohibitiva que s'hi conté, i en el proemi de la disposició legislativa del Govern només consta una argumentació genèrica que invoca la manca de dades o de coneixement sobre la tecnologia vetada, alhora que manté la prohibició «mentre no hi hagi més dades o un marc regulador *ad hoc* de caràcter estatal o europeu que faci front a les debilitats que implica el seu ús per a les dades i la seguretat pública».

En relació amb la manca de coneixement esmentada, abans de prohibir de forma absoluta una tecnologia, que no és negativa en si mateixa i té avantatges, es pot testar de forma parcial. És evident que són imaginables altres fórmules que permetin equilibrar el principi de precaució i el d'innovació i que serien molt més respectuoses i menys lesives amb la competència d'autoorganització de les administracions públiques que no pas optar per la prohibició, sense més ni més, d'una tecnologia —que té una varietat molt àmplia d'aplicacions— per donar suport als instruments administratius propis.

Altrament, quant als sistemes d'identificació i de signatura electròniques, el legislador estatal bàsic (art. 149.1.18 CE) ja garanteix aquest tractament comú, entre d'altres, quan imposa l'acceptació per part de totes les administracions dels sistemes que considera que tenen major nivell de seguretat o confiança (art. 9.2.*a*, .*b* i .*c*, segon paràgraf, i art. 10.2.*a*, .*b* i .*c*, segon paràgraf, LPACAP) (STC 55/2018, FJ 9) i, a més, ha aprovat també un conjunt de previsions bàsiques en matèria de seguretat (l'esmentat Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica).

Un cop exposats els documents d'investigació i anàlisi anteriors, cal resoldre si les «debilitats» de les TRDs al·legades al preàmbul del Reial decret llei justifiquen la prohibició continguda a la nova disposició addicional sisena LPACAP.

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

En segon lloc, aquestes debilitats no semblen justificar la prohibició d'una concreta tecnologia per part de l'Estat, ja que el compliment del RGPD no és qüestió de la tecnologia, sinó de com és utilitzada aquesta. Si es volen limitar els possibles problemes jurídics que poden ocasionar determinades TRDs, el que pot fer aquest és establir cauteles i normes de mínims, que després podran ser desenvolupades pel legislador autonòmic.

Finalment, les TRDs ofereixen avantatges importants per a la posada en marxa de projectes de governança política, àmpliament tractats a un estudi europeu de recerca i assessorament a la Comissió Europea titulat *Blockchain for digital government* (2019), que recomana, en el mateix sentit que la Resolució del Parlament Europeu, de 3 d'octubre de 2018, fer proves pilot d'aquesta tecnologia.

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

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

El legislador estatal introdueix aquesta prohibició sense ser estrictament necessària o idònia. Tampoc no explicita suficientment les raons que justifiquen dictar una norma prohibitiva d'aquesta mena, en comptes de fixar, podent-ho fer, un marc regulador bàsic, que concreti o afegeixi requisits addicionals de seguretat o de protecció de dades als que ja ordenen el Reglament eIDAS i el Reglament europeu de protecció de dades, per evitar els eventuals problemes que l'esmentat preàmbul del Reial decret llei apunta sense detallar. Es tracta d'un ús espuri i desproporcionat del títol competencial de l'article 149.1.18 CE per suplir una mancança que en realitat és atribuïble al mateix Estat, que no s'ha dotat d'un marc regulador bàsic.

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

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

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

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

Des d'una perspectiva material, l'esmentada previsió normativa genera un marc confús i susceptible d'interpretacions diverses, que no precisa el seu abast ni els seus efectes, raó per la qual no és pot titllar d'inconstitucional tot i que cal afirmar que és un exemple de mala tècnica legislativa.

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

El nou article 4.6 LGTEL atribueix al Govern de l'Estat una facultat general consistent en la capacitat per acordar la gestió directa o la intervenció de les xarxes i els serveis de comunicacions electròniques en determinats supòsits articulats al voltant de tres conceptes jurídics indeterminats (ordre públic, seguretat pública i seguretat nacional), 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.

Es tracta d'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 es pot 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 s'ha de 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». En aquest sentit, 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. No es pot ignorar que les xarxes i els serveis de comunicacions electròniques constitueixen la via d'entrada als continguts i a la societat de la informació ni, per tant, la convergència d'ambdós sectors i els vincles que existeixen entre ells (considerants 7 i 10 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).

En paraules més sintètiques, hom pot dir que es tracta d'internet i dels diferents nivells de connectivitat que aquesta xarxa global permet. De fet, 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 més o menys intensitat, amb les comunicacions electròniques, que es consideren més un nou paradigma cultural, inclòs el seu vessant polític, que no pas un mer instrument o mitjà de comunicació més.

Quant als conceptes d'ordre públic, seguretat pública i seguretat nacional, amb les corresponents modulacions i a tall de resum, 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.

D'entrada, aquesta conformació de l'article 4.6 LGTEL 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 de comunicacions electròniques, els quals simultàniament són establerts com a objectiu i pressupòsit habilitant. La combinació d'una enorme discrecionalitat del 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 que hi operen, junt amb l'absència de previsió de cap mena de delimitació funcional ni tampoc 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 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'intervindria 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), 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.

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», que la norma no precisa ni delimita (no és objecte d'examen l'assumpció per part d'aquesta de la gestió directa de l'explotació de les xarxes i de la prestació dels serveis de comunicacions electròniques, acotada per la legislació de la contractació pública i 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), 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 (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»). 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).

Tots els elements de la configuració de la norma apuntalen la interpretació de la clàusula genèrica i imprevisible. Defectes, aquests, de 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 «[e]ls 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, «[c]om 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, «[a]ixí, 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).

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.

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, esdevé cabdal recordar que 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 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» (assumpte *Ahmet Yildirim contra Turquia*, STEDH 3111/10, de 18 de desembre de 2012, resultant definitiva el 18 de març de 2013, 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 doctrina constitucional, quan 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» *ex* article 9.3 CE (STC 169/2001, de 16 de juliol, FJ 6). 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, 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).

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 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, 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*).

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, es conclou que 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 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 objecte del Dictamen, atès que la primera condició de validesa, la qualitat de la llei, 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.

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.

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 i l'article 15.1 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.