Les tecnologies de la informació i de la comunicació a Catalunya

Generalitat de Catalunya
Consell Assessor
per a la Transició Nacional

Les tecnologies de la informació i de la comunicació a Catalunya

Generalitat de Catalunya
Consell Assessor per a la Transició Nacional

Índex

Les tecnologies de la informació i de la comunicació a Catalunya

1. Objecte de l'informe

L'objecte d'aquest informe és doble. D'una banda, analitza els riscos relacionats amb la seguretat de les comunicacions electròniques, així com les estratègies i mesures que el Govern de la Generalitat hauria d'adoptar en el procés de Transició Nacional per fer-hi front. I, de l'altra, planteja les mesures que caldria prendre per tal de subrogar-se en la posició que ocupa l'Estat en relació amb les TIC que són avui de titularitat o que gestiona l'Estat espanyol.

L'informe constata la importància vital que han assolit les tecnologies de la informació i de la comunicació (en endavant les TIC) en les societats modernes i la necessitat consegüent de garantir en tot moment el seu funcionament i, de manera molt especial, el de les que denominem estructures crítiques per la seva transcendència estratègica en la vida d'aquestes societats.

A partir d'aquesta constatació inicial, analitza els elements que cal tenir en compte a l'hora de detectar els riscos que poden amenaçar el funcionament normal de les TIC i, al mateix temps, prendre les mesures necessàries per garantir aquest funcionament durant el procés de Transició Nacional i els primers mesos de funcionament del nou Estat, naturalment si la seva constitució fos l'opció adoptada pels ciutadans de Catalunya.

Analitzats els riscos des de la triple perspectiva de les competències i la seguretat física i cibernètica de les infraestructures, l'informe passa a examinar els principals actius a protegir, tot distingint, en cada cas, els escenaris de col·laboració i no-col·laboració amb l'Estat.

En el darrer epígraf es fa referència a les comunicacions basades en Internet i xarxes socials que, com és sabut, tenen un paper cada vegada més rellevant com a mitjà d'informació i comunicació.

2. La importància de la seguretat i de les tecnologies de la informació i les comunicacions

Les infraestructures relacionades amb les TIC són necessàries per al bon funcionament dels serveis bàsics destinats a la població i dels sistemes de producció de la nostra societat. Qualsevol interrupció no desitjada, ja sigui causada per desastres naturals, fallades tècniques o atacs deliberats, tindria greus conseqüències en el funcionament dels serveis o en els fluxos de subministrament.

L'alt grau de desenvolupament de les societats occidentals suposa al mateix temps una feblesa. Les societats desenvolupades i altament tecnificades depenen en extrem d'una sèrie de serveis anomenats essencials, sense els quals no se'n pot garantir la subsistència: aigua, electricitat, sistemes de transport, telecomunicacions, etc. Es tracta de serveis que requereixen infraestructures crítiques, en el sentit que el seu funcionament esdevé indispensable per garantir-ne la provisió i no permeten solucions alternatives, per la qual cosa la seva pertorbació o destrucció tindria un greu impacte sobre els serveis essencials. Per això mateix, han de ser objecte d'una especial protecció.

En l'actualitat hi ha multitud de reptes que afecten la seguretat d'aquestes infraestructures. Per aquest motiu, i en el marc de les prioritats estratègiques dels estats, es fa imprescindible, d'una banda, la identificació i catalogació d'aquestes prioritats i, d'una altra, dissenyar plans que prevegin les mesures més eficaces de prevenció i protecció destinades a reduir, i fins i tot anul·lar, els perills que afecten aquestes infraestructures.

L'àmbit de les TIC no és aliè a aquesta situació. Les TIC agrupen els elements i les tècniques utilitzats en el tractament i la transmissió de la informació, la informàtica, Internet i les telecomunicacions. Les TIC abasten dos tipus d'infraestructures:

- Els sistemes d'informació: conjunt d'infraestructures i tecnologies que emmagatzemen informació i dades;
- Les xarxes de comunicació: conjunt d'infraestructures i tecnologies que transporten aquestes dades.

Per tant, com qualsevol altra infraestructura (viària, ferroviària, de sanejament, aèria, etc.) les infraestructures de les TIC també es dissenyen per proporcionar connectivitat, en l'esfera de les comunicacions electròniques. A més, en la mesura que també representen una infraestructura crítica, requereixen polítiques actives que les protegeixin i les dotin dels mecanismes de seguretat que garanteixin la seva disponibilitat. Tanmateix, les infraestructures de les TIC esdevenen molt més vulnerables pel fet que estan interconnectades i en depèn el bon funcionament d'altres infraestructures físiques, tant en els sistemes d'informació, com en les seves xarxes de comunicació.

Connectivitat, disponibilitat i seguretat són els factors determinants a l'hora d'entendre el funcionament d'aquesta mena d'infraestructures i de garantir la continuïtat dels serveis que presten.

Durant el procés de Transició Nacional, un dels primers i més importants reptes hauria de ser el de mantenir la continuïtat de les TIC necessàries per al funcionament dels serveis del nostre país.

Garantir la continuïtat dels sistemes d'informació i les xarxes de telecomunicacions seria relativament fàcil si hi ha voluntat de col·laboració tant per part del govern de l'Estat espanyol com dels operadors privats en telecomunicacions. Un entorn de col·laboració amb l'Estat podria permetre que aquest fes el traspàs de competències i responsabilitats de gestió de forma ordenada i sense posar en risc els serveis. En aquest traspàs també es podrien tenir en compte els aspectes econòmics associats a les autoritzacions de l'ús de l'espectre que les operadores aporten a l'Estat i que, a partir de cert moment, eventualment gestionaria el govern del nou Estat. Naturalment, en cas de no-col·laboració, la tasca de la Generalitat per assolir la continuïtat dels serveis amb forta dependència TIC esdevindria més complexa.

3. Els aspectes de les TIC a tenir en compte durant el procés de Transició Nacional

Com ja s'ha esmentat, existeixen uns riscos que poden posar en perill el correcte funcionament de les infraestructures TIC. Aquests riscos són els que cal valorar a l'hora de treballar conjuntament amb l'Estat espanyol, per tal que no esdevinguin un impediment real per a la continuïtat dels serveis de telecomunicacions. Aquesta valoració s'ha de fer essencialment en relació amb tres aspectes:

- Les competències i els contractes: l'Estat espanyol té competències sobre els serveis de comunicacions, algunes infraestructures crítiques i, en conseqüència, sobre les empreses privades que gestionen els serveis associats. L'Estat té competències que li permeten garantir les infraestructures crítiques en àmbits com l'Administració pública, l'aigua, l'alimentació, l'energia, l'espai aeri, la indústria química, la indústria nuclear, les instal·lacions d'investigació, la salut, el sistema financer i tributari, les tecnologies de la informació i les comunicacions, o els transports. A més, és el titular de les radiofreqüències, de l'Autoritat aeroportuària, de l'espai aeri, entre d'altres. Seria essencial poder garantir que, durant el traspàs de les competències i contractes, no quedin buits legals ni buits de servei que afectin el funcionament normal del país.
- La seguretat física: tant en un escenari de col·laboració com de no-col·laboració caldria que ambdós governs vetllessin per la integritat física de les infraestructures.
- La seguretat cibernètica: les infraestructures TIC també es podrien veure amenaçades per atacs informàtics. Aquesta mena d'atacs constitueixen el risc que cal tenir més en compte, no només pel mal que poden provocar sinó perquè, en ser una actuació silenciosa i anònima, la seva autoria és difícil de demostrar. Tanmateix, tot Estat disposa de serveis d'intel·ligència que poden actuar a través d'Internet a favor i en defensa dels seus interessos. Per tant, caldria col·laborar amb l'Estat espanyol per poder rebutjar actuacions bel·ligerants a través de la

xarxa contra les infraestructures TIC. Les actuacions bel·ligerants a través de la xarxa s'englobarien en el concepte de "ciberseguretat".

4. La seguretat lògica: la ciberseguretat

4.1. Descripció

Les comunicacions i les infraestructures crítiques que les suporten tenen un alt nivell de dependència de l'aspecte tecnològic. Per aquesta raó, a banda dels atacs de tipus físic, la legislació europea considera els atacs de tipus lògic, comunament plantejats sota el concepte de ciberseguretat.

Fins ara, els tecnòlegs s'han orientat a l'eficàcia en l'operació d'aquests sistemes i a la creació de serveis amb importants beneficis per a la societat; ara, però, el nou repte és la protecció d'aquests beneficis. Cal protegir especialment la xarxa dels virus, cucs, zombis, hackers i la resta d'amenaces conegudes. A tall d'exemple, el Centre de Seguretat de la Informació de Catalunya (CESICAT) arriba a aturar al voltant de 2 milions d'incidents mensuals.

Cal preveure, doncs, la possibilitat d'atacs o sabotatges dirigits contra la xarxa per tal d'intentar paralitzar les infraestructures de comunicacions, CPD, sistemes d'informació, energia, mitjans de comunicació, serveis financers, logístics o de distribució d'energia, aigua o gas. Avui dia, tots aquests serveis estan connectats a la xarxa i no poden funcionar sense aquesta, de manera que són vulnerables, en major o menor mesura, als atacs dels ciberdelinqüents o hackers.

En conseqüència, cal preparar-se per actuar com un antivirus en tot aquest procés, i reforçar-ne la protecció. A hores d'ara, les infraestructures catalanes estan protegides pels CERT[1], integrats per persones, màquines i programes que en garanteixen la protecció vint-i-

[1] CERT és l'acrònim de *Computer Emergency Response Team*, o el que és el mateix, Equip de Resposta a Incidents Informàtics.

quatre hores al dia, els set dies de la setmana. En l'àmbit de la Generalitat hi ha més de 100.000 ordinadors i milers de servidors i equips de comunicacions –en total al voltant de 300.000 màquines– que fan que el dia a dia funcioni. En aquests casos de xarxes complexes només es poden protegir aquests entorns amb eines automatitzades controlades per persones que les vigilen contínuament. Catalunya disposa d'una entitat, el CESICAT, que en té la responsabilitat.

Malgrat que Catalunya disposa des de l'any 2009 d'un Pla nacional d'impuls de la seguretat de les TIC a Catalunya, el seu desplegament és encara incomplert des de la perspectiva de les amenaces existents en el ciberespai. Les limitacions i delimitacions geopolítiques, la multiplicitat d'agències i competències a nivell europeu, estatal i autonòmic, compliquen l'escenari i per aquesta raó, caldria que Catalunya preveiés una estratègia en ciberseguretat i desenvolupés la seva capacitat de protecció dels interessos privats i públics contra les amenaces del món virtual.

4.2. La ciberseguretat lògica en el context internacional i europeu

La Unió Europea està liderant el desenvolupament d'una estratègia de seguretat europea mitjançant l'Agenda Digital, que dóna cobertura, en el *Pilar III Trust and Security*, a les accions directrius per als temes de ciberseguretat i privacitat en la xarxa. L'estratègia en ciberseguretat a la Unió Europea i la proposta de Directiva europea sobre mesures per a l'assoliment d'un nivell comú més elevat en la seguretat de la xarxa i de la informació defineixen un marc programàtic on encabir la nova creació d'organismes, com l'*European Cybercrime Centre* (EC3), l'Oficina Europea per a la Lluita contra el Frau (OLAF), el *Computer Emergency Response Team* (CERT-EU), l'organisme per a la protecció de les infraestructures crítiques, *l'European Public-Private Partnership for Resilience* (EP3R) o l'Agència Europea de la Seguretat de la Xarxa i les Informacions (ENISA).

Els mateixos països europeus estan desplegant diferents estratègies, polítiques i organismes per a donar resposta a les seves necessitats nacionals de protecció.

Així mateix, l'OTAN considera que la segona amenaça potencial en la seguretat dels països

membres, després d'un atac nuclear, és l'atac a la xarxa. Així es va explicitar a la *Chicago Summit Declaration* del maig de 2012[2].

Al gener de 2011, segons les autoritats canadenques, els sistemes de contrasenyes del Ministeri de Finances van ser víctimes d'un ciberatac procedent de màquines instal·lades a la Xina.

4.3. La ciberseguretat lògica a Catalunya

Catalunya ha estat capdavantera a Espanya en la creació de centres de resposta a incidents

[2] Exemples d'atacs informàtics:

2011 – El Canadà atacat des de la Xina

Al gener de 2011, segons les autoritats canadenques, els sistemes de contrasenyes del Ministeri de Finances van ser víctimes d'un ciberatac procedent de màquines instal·lades a la Xina.

2010 – Iran

A finals de setembre de 2010, l'Iran també va registrar un atac a les centrifugadores del programa d'enriquiment d'urani -programa nuclear iranià-. El troià, virus o programa infiltrat va rebre el nom de Stuxnet.

2008 – Geòrgia

A l'agost de 2008, durant el conflicte bèl·lic de Rússia, Ossètia del Sud (Geòrgia) es van produir ciberatacs per part de Rússia, orientats cap a llocs governamentals.

2007 – Estònia

El 2007 Estònia va culpar les autoritats de Rússia de diversos atacs continuats que van afectar a mitjans de comunicació, bancs i diverses entitats i institucions governamentals. Actualment la seu de l'organisme de ciberdefensa de l'OTAN està situada a Estònia.

2003 – Taiwan

El 2003, Taiwan va rebre un possible atac del qual va culpar les autoritats de la Xina. No n'hi ha proves, però va deixar sense servei infraestructures com ara hospitals, la Borsa i alguns sistemes de control de trànsit. El suposat atac va provocar un caos progressiu i amb una aparent organització que, a més d'un atac de denegació de servei, va incloure virus i troians.

Actualment la unitat encarregada de la ciberdefensa xinesa és una unitat de l'exèrcit comandada per un general i compta amb 20.000 efectius coneixedors de tots els idiomes, inclòs el català.

1999 Kosovo

Els ciberatacs també van jugar un paper important durant la intervenció dels aliats en la guerra de Kosovo.

(CERT), agències de protecció de dades (Apdcat), certificats digitals (Catcert) i desplegament de l'estratègia de seguretat (CESICAT).

En aquest marc, a l'hora de dissenyar futurs plans o estratègies de ciberseguretat, caldria tenir presents els objectius a protegir, els eixos d'actuació i les funcions de la ciberseguretat següents.

4.3.1. Els objectius de protecció de ciberseguretat

Un eventual document que consideri, en forma d'estratègia o de document similar, la ciberseguretat a Catalunya hauria de cercar almenys els objectius de protecció següents: a) les comunicacions del Govern i dels serveis públics; b) les infraestructures crítiques i el seu entorn TIC; i c) les dades dels ciutadans. Tot plegat, impulsant la confiança i seguretat en les TIC de ciutadania i Administració.

Concretament, la protecció de les comunicacions del Govern i dels serveis públics s'orienta a garantir tant les comunicacions que rep la població, de forma regular i contínua, per tal de satisfer certes necessitats d'interès general, com les comunicacions internes i com, finalment, els serveis bàsics de les administracions. Cal recordar que les TIC donen suport al correcte desenvolupament d'aquests serveis i esdevenen el mitjà principal per al govern electrònic, l'administració electrònica i la participació ciutadana.

Pel que fa a la protecció de les infraestructures crítiques, n'hi hauria prou a reiterar que d'aquestes depenen el bon funcionament i la fiabilitat en la prestació de determinats serveis, alguns de primera necessitat, com l'aigua, la sanitat o l'energia. Qualsevol mal funcionament d'aquests serveis, encara que fos per un breu espai de temps, tindria conseqüències greus i imprevisibles.

Finalment, pel que fa la protecció de les dades dels ciutadans, recordem que la seva gestió, explotació i tractament són cabdals per a la provisió dels serveis públics. A més, contenen informació sensible i que cal protegir (diu qui som, quines capacitats i habilitats tenim, estudis, salut...). Caldria, doncs, assegurar el seu ús, però també la seva protecció, que constitueix un dret fonamental.

4.3.2. Els eixos d'actuació de la ciberseguretat

Són quatre els eixos principals d'actuació que permeten desenvolupar els objectius que s'acaben d'exposar. Naturalment, alguns d'aquests eixos estan relacionats amb altres polítiques públiques vinculades a la seguretat i a la defensa, per la qual cosa, caldria establir les corresponents sinergies i coherència entre polítiques públiques. Per tant, ens limitem a enumerar els eixos d'actuació o dimensions que en principi caldria considerar.

- Govern i serveis a la societat

Caldria garantir la seguretat del ciberespai català vinculat a la capacitat i viabilitat del Govern i l'Administració per a dur a terme les seves funcions. Per tant, les actuacions s'haurien d'orientar a la protecció de la xarxa i de la informació del Govern i l'Administració, així com a la definició i la promoció d'estàndards de seguretat i la seva translació a la compra pública de TIC.

- Intel·ligència

Per intel·ligència s'entén en les societats modernes el conjunt de resultats derivats d'avaluar, integrar i analitzar informacions sensibles, segons el context prèviament definit, i la seva conversió, mitjançant diversos instruments, en coneixement útil.

Els dominis d'intel·ligència creixen constantment al món actual i es poden diferenciar en dos grans apartats: intel·ligència civil o de govern i intel·ligència de seguretat, que inclou el subcomponent militar. També s'utilitza el concepte d'informació.

En el cas que ens ocupa, el ciberespai, hom busca generar intel·ligència sobre intencions, operacions i capacitats internes i externes.

- Seguretat i defensa

Inclou, en el camp del ciberespai, la capacitat de generar protecció i prevenció contra la totalitat d'amenaces imminents i la robustesa de l'entorn TIC actual i futur. En aquest punt, la distinció entre seguretat i defensa queda difuminada. En tot cas, de comú acord amb les eventuals estratègies de seguretat, caldria "securitzar" els interessos nacionals, tot preservant –amb mesures diverses de contenció i protecció– les infraestructures crítiques i el

rebuig d'atacs cibernètics contra els esmentats interessos. A tall d'exemple, la protecció busca disposar de filtres que rebutgin les comunicacions procedents de dispositius catalogats (en funció de dades d'intel·ligència) com a perillosos o procedents de llistes negres contrastades.

- Forces de l'ordre

Com és obvi, la ciberseguretat implica una relació estreta amb les forces d'ordre públic, per tal de prevenir, perseguir i detenir persones o organitzacions que cometen delictes. Naturalment, la tasca bàsica és el cibercrim, és a dir, els delictes informàtics, una tasca que implica respecte a l'Estat de dret i col·laboració amb el poder judicial.

4.3.3. Les funcions de la ciberseguretat

Per garantir un desenvolupament correcte de la ciberseguretat, cal implementar un seguit de funcions comunes, però també cal preveure funcions específiques per a cadascun dels quatre eixos d'actuació. Concretament:

- Funcions comunes o generals:

  Entre d'altres, col·laboració, monitorització, resposta a incidents, difusió de resultats i generació d'informes, recollida d'informació, anàlisi de la informació, exercici i formació.

- Funcions específiques per a cada eix d'actuació:

  El quadre que segueix presenta els 4 eixos i algunes funcions pròpies de cadascun d'ells, que s'expliciten posteriorment. Per facilitar la comprensió, les enumerarem per funcions, indicant-ne en cada cas els eixos d'actuació que en resulten afectats.

Taula 1. Funcions de ciberseguretat específiques de cada eix d'actuació

Govern i serveis a la societat	Intel·ligència
• Estratègia • Protecció de sistemes • Coordinació público-privada • Coordinació de la intel·ligència exterior	• Recerca i desenvolupament • Qualificació de les amenaces i identificació dels atacs • Coordinació de la intel·ligència exterior
Seguretat i defensa	**Forces d'ordre públic**
• Recerca i desenvolupament • Investigació • Interrupció d'activitats il·lícites • Coordinació público-privada	• Estratègia • Investigació • Interrupció d'activitats il·lícites

Més específicament:

- Estratègia

Funcions que afecten el Govern i els serveis que presta l'Administració a la societat i les forces d'ordre públic. Cal considerar les funcions actuals, atribuïdes des de la seva creació al CESICAT, i les que en el futur es puguin atribuir al Govern i a l'Administració. També cal definir estratègies compartides en la lluita contra el ciberdelicte (forces d'ordre públic).

- Recerca i desenvolupament

Les tasques de recerca i desenvolupament afecten fortament, atesa la relació amb la intel·ligència, els principals problemes de seguretat o d'anàlisi de la informació.

En el camp de la seguretat i de la defensa, el principal factor a tenir en compte és que les tecnologies TIC estan evolucionant constantment i exponencialment en relació amb allò que pot afectar les amenaces, els riscs, la vulnerabilitat i les eines per a tractar-les. Altrament dit,

la detecció i la resposta d'un atac potencial requereixen, atesa l'evolució tecnològica, capacitat de recerca i desenvolupament de noves eines i solucions.

- Qualificació de les amenaces i identificació dels atacs

Al·ludim a una funció, vinculada amb la intel·ligència, que dóna suport a la resta d'eixos d'actuació i, especialment, a la relacionada amb les forces d'ordre públic, atès que identificar i qualificar de forma primerenca una amenaça o atac (per tant, la correcta identificació, atribució i origen de l'amenaça o l'atac) són clau per a la seva resolució positiva.

- Investigació

La investigació és consubstancial a la tasca dels cossos policials, tant per a investigar delictes informàtics com per a funcions pericials. Quant a la seguretat, calen capacitats molt evolucionades (Forense Digital) per poder determinar les accions portades a terme per eventuals atacants, les debilitats pròpies i la capacitat de persistir en els atacs. Aquest capacitat forense s'ha de posar a disposició de les forces d'ordre públic.

- Interrupció d'activitats il·lícites

Resulten òbvies per a les forces d'ordre públic (evitar o aturar un delicte informàtic quan aquest s'està portant a terme) i per a la seguretat (estar en condicions de detectar i contenir un eventual atac a un servei o infraestructura crítica).

- Protecció de sistemes

Actualment en té competències el CESICAT, però se'n poden atribuir a d'altres instàncies.

- Coordinació públic-privada

Afecta a l'eix del Govern i a la prestació de serveis a la societat civil, atès que la relació amb l'entorn privat és pròpia del Govern i l'Administració, i també a l'eix de la seguretat i de la defensa.

- Coordinació de la intel·ligència exterior

Les funcions d'intel·ligència avui estan força internacionalitzades, amb àmbits de cooperació i, per tant, caldrà assegurar aquesta coordinació i la corresponent tramesa d'informació.

4.4. Escenaris de col·laboració i riscos

Catalunya hauria de desplegar una estratègia integral per tal de fer front a la lluita contra les diferents i múltiples tipologies de ciberamenaces que existeixen a tot el món i que tenen una tendència creixent.

Així mateix, en el progressiu desplegament de capacitats en ciberseguretat per part de l'Administració catalana en el moment de la Transició Nacional, caldria mantenir la ja existent col·laboració amb organismes de l'Estat espanyol, com ara, l'*Instituto Nacional de Tecnologías de la Comunicación (*INTECO) i el *Centro Criptológico Nacional* (CCN-CERT), així com d'altres organismes a nivell europeu, com ara el Centre de Resposta a Incidents (CERT-EU) o l'Agència Europea de la Seguretat de la Xarxa i les Informacions (ENISA). Cal ser conscients que qualsevol grup de ciberactivistes (hackers) contraris al procés podria dur a terme actuacions bel·ligerants contra els sistemes de la Generalitat o les infraestructures crítiques. L'escenari seria òbviament més complex en un context de no-col·laboració o bel·ligerància.

4.5. Alternatives

Caldria que Catalunya desplegués una estratègia en ciberseguretat, amb polítiques i una organització adequades, i on les capacitats de defensa i prevenció fossin clau i on aquestes capacitats poguessin adoptar accions de contenció si fos necessari per a la seguretat dels sistemes.

Dins de l'estratègia de seguretat, cal fer especial esment a la protecció de les infraestructures crítiques per tal d'evitar casos com els descrits anteriorment.

5. El marc legal de les TIC

5.1. El marc competencial i les telecomunicacions

Malgrat que les comunicacions electròniques funcionen en un mercat liberalitzat seguint normatives de la Unió Europea (UE), cada Estat regula el marc legal aplicable al seu territori. A l'Estat espanyol les telecomunicacions es troben regulades en la Llei 32/2003, de 3 de novembre, general de telecomunicacions (LGTEL), la qual ha de ser respectada per tots els operadors. En aquesta Llei es regulen, entre d'altres, el servei universal que fixa els drets dels ciutadans a rebre serveis mínims, l'adjudicació de l'espectre per operar xarxes mòbils o els serveis de ràdio i els títols habilitants per a operadors de xarxes. En tot cas, cal tenir present que el Govern espanyol té previst aprovar una nova llei de telecomunicacions que pot alterar en bona mesura el marc jurídic actual.

La creació d'un nou Estat implicaria l'aprovació de noves lleis com a resultat de la seva sobirania i la seva capacitat de regulació. Val a dir que l'entorn de col·laboració amb l'Estat espanyol seria essencial per a dur a terme un traspàs competencial i establir un marc jurídic que donés seguretat als operadors durant el procés.

La creació d'un nou marc legal en telecomunicacions no es produiria de forma immediata l'endemà d'una eventual constitució del nou Estat català. El marc legal del dia després de la creació del nou Estat s'hauria de regir, d'entrada, pel principi de continuïtat que pressuposaria que els operadors mantindrien els seus títols habilitants, és a dir, els seus drets d'ús de l'espectre radioelèctric que fan possible les xarxes mòbils. Així, doncs, el marc legal continuaria sent la LGTEL, ja que caldria evitar situacions de buit legal que afectessin els serveis als ciutadans i empreses. Tot i això, a mitjà termini l'exercici sobirà de creació d'un nou marc legal seria irrenunciable. Aquesta situació i la pròpia capacitat del nou Estat d'aplicar sancions per incompliments dels contractes dels operadors faria que la continuïtat dels serveis no es veiés amenaçada.

5.2. Les comunicacions electròniques: el marc de regulació europeu

L'any 1997 la Comissió Europea iniciava un període de reflexió en relació amb les implicacions, sobretot d'ordre jurídic, que suposava la convergència entre els sectors de telecomunicacions i de l'audiovisual així com la publicació d'un Llibre Verd sobre la convergència dels sectors de telecomunicacions, mitjans de comunicació i tecnologies de la informació i sobre les seves conseqüències per a la reglamentació, dins de la perspectiva de la societat de la informació europea. Calia, dins d'aquesta perspectiva, adaptar els marcs reguladors existents en aquell moment al nou entorn tecnològic. Avui, podem dir que la convergència tecnològica és ja una realitat.

Una de les adaptacions necessàries, fruit de la convergència tecnològica, va ser la modificació de l'objecte de regulació. El nou marc regulador, aprovat per la Unió Europea el 2009, ja no té en compte només les telecomunicacions, la televisió i Internet, sinó que ha establert un marc regulatori adaptat al nou entorn: les comunicacions electròniques.

La Unió Europea ha adoptat normatives, i n'adoptarà de noves, destinades al bon funcionament del mercat interior europeu de les comunicacions. El darrer exemple és una proposta de Reglament de la UE per a la reducció de costos de desplegament de xarxes de comunicacions electròniques de banda ampla.

Però la Unió Europea no té competències en tots els àmbits i en tot cas persegueix la regulació unitària del mercat interior europeu a través de l'harmonització de les normatives dels Estats membres. Per aquesta raó, i davant la creació d'un nou Estat, caldrà adoptar una nova Llei general de les comunicacions electròniques que complementi les necessitats de funcionament del mercat interior europeu amb els objectius de desenvolupament de la nostra economia, territori i cultura dins del nou entorn de l'economia digital.

5.3. Les infraestructures crítiques: objecte de protecció prioritària

Després dels esdeveniments de l'11 de setembre de 2001 l'escenari de la seguretat mundial

va patir canvis significatius. A partir d'aquest moment es van fer paleses les implicacions que la destrucció o alteració de certs objectius podrien tenir sobre la vida, la salut i el benestar dels ciutadans i el funcionament dels estats. S'inicia un nou tractament de la seguretat sobre aquests objectius, es deixa de banda el concepte tradicional i se n'incorpora un altre de completament nou. Efectivament, fins a aquella data la seguretat era una competència pública i exclusiva de l'Estat. Ara es té present que les infraestructures crítiques estan majoritàriament en el sector privat, i per tant, aquest sector n'és també responsable.

En el cas dels Estats Units i després de l'11S es va reaccionar amb la creació del Departament de Seguretat Interior i una nova i àmplia regulació en aquesta matèria. A nivell europeu, la iniciativa va sorgir sobretot arran dels atemptats a Madrid de l'11 de març de 2004.

A partir d'aquests primers passos, la Comissió Europea va elaborar una estratègia global sobre protecció d'infraestructures crítiques, amb propostes per millorar la prevenció, la preparació i la resposta dels estats europeus enfront d'atemptats terroristes.

Posteriorment va aprovar-se la Directiva 2008/114/CE del Consell de 8 de desembre de 2008 sobre la identificació i la designació d'infraestructures crítiques europees i l'avaluació de la necessitat de millorar la seva protecció, la qual va entrar en vigor el 12 de gener de 2009.

Aquesta Directiva estableix, entre d'altres coses, que la responsabilitat principal i última de protegir les infraestructures crítiques correspon als Estats membres i als operadors d'aquestes, i insta a la implantació d'una sèrie d'iniciatives i actuacions per part dels Estats per a la seva transposició a les legislacions nacionals.

5.4. El sector TIC: legalitat vigent a l'Estat espanyol

El marc legal en matèries diverses ha evolucionat en una complexa combinació d'estatuts i regulacions legals, regles judicials i la pràctica real. Tanmateix, no és estrany trobar llacunes, conflictes i inconsistències entre les diferents parts que donen forma a un marc legal i en conseqüència al procés en si.

Com en d'altres àmbits materials, el marc legal estatal relatiu al sector de les TIC ha experimentat un canvi notable, no exempt de llacunes i inconsistències, provocades en part pel fet que es tracta d'un sector caracteritzat per la celeritat de l'actualització tecnològica.

Així mateix, cal tenir en compte que els serveis de comunicació audiovisual (radiofònics, televisius i connexos i interactius) són serveis d'interès general que es presten en l'exercici del dret a la lliure expressió d'idees i del dret a comunicar i rebre informació, entre d'altres (art. 22.1 de la Llei 7/2010, de 31 de març, general de la comunicació audiovisual - LGCA). En conseqüència, la prestació d'aquests serveis resta lligada a l'exercici de drets reconeguts constitucionalment (art. 20.1a i d de la CE) de manera que una eventual impossibilitat de prestar els serveis de comunicació audiovisual podria comportar la vulneració d'aquests drets. Això no obstant, la mateixa CE estableix mecanismes per poder suspendre el seu exercici tot declarant l'estat d'excepció o de setge (art. 55.1). Per tant, i també d'acord amb els art. 21 i 32.3 de la Llei orgànica 4/1981, d'1 de juny, dels estats d'alarma, excepció i setge (LOEE), no s'hauria de descartar que això pogués afectar el funcionament correcte de les emissions de ràdio i televisió, entre d'altres. Aquest supòsit només es podria produir, lògicament, en l'etapa prèvia a la constitució de l'Estat català[3].

[3] En efecte, l'article 55.1 de la CE estableix que els drets reconeguts en l'article 20, apartats 1 a) i d), entre d'altres, podran ser suspesos quan sigui acordada la declaració de l'estat d'excepció o de setge en els termes que preveu la CE. Així, l'apartat 3 de l'article 116 de la CE determina que l'estat d'excepció serà declarat pel Govern mitjançant un decret acordat en un Consell de Ministres, prèvia autorització del Congrés dels Diputats. L'autorització i la proclamació de l'estat d'excepció haurà de determinar expressament els efectes d'aquest, l'àmbit territorial al qual s'estengui i la durada, que no podrà excedir de trenta dies, prorrogables per un termini igual amb els mateixos requisits.

D'acord amb l'article 13 de la LOEE, el Govern podrà sol·licitar del Congrés dels Diputats autorització per declarar l'estat d'excepció "cuando el libre ejercicio de los derechos y libertades de los ciudadanos, el normal funcionamiento de las instituciones democráticas, el de los servicios públicos esenciales para la comunidad, o cualquier otro aspecto del orden público, resulten tan gravemente alterados que el ejercicio de las potestades ordinarias fuera insuficiente para restablecerlo y mantenerlo" (apartat 1). A aquests efectes, el Govern remetrà al Congrés una sol·licitud d'autorització que contindrà els extrems següents (apartat 2):

- "Determinación de los efectos del estado de excepción, con mención expresa de los derechos cuya suspensión se solicita, que no podrán ser otros que los enumerados en el apartado 1 del art. 55 de la Constitución.
- Relación de las medidas a adoptar referidas a los derechos cuya suspensión específicamente se solicita.
- Ámbito territorial del estado de excepción, así como duración del mismo, que no podrá exceder de treinta días.

Per la seva banda, en relació amb el sector de les telecomunicacions la Llei 32/2003, general de telecomunicacions, estableix les principals condicions sota les quals les entitats privades poden prestar serveis de telecomunicacions i regula també les condicions en les quals el Govern i les principals institucions estatals gestionen i regulen un servei d'interès públic i, en relació amb el cas d'estudi, a l'article 4 preveu que:

"*1. Las redes, servicios, instalaciones y equipos de telecomunicaciones que desarrollen actividades esenciales para la defensa nacional integran los medios destinados a ésta, se reservan al Estado y se rigen por su normativa específica*".

És rellevant mencionar aquesta disposició principalment pel fet que no totes les d'infraestructures de telecomunicacions queden sotmeses al règim de la LGTEL sinó que n'hi ha que queden reservades a l'Estat i tenen com a finalitat la defensa nacional, principalment infraestructures de caire militar o d'infraestructures crítiques. Cal tenir en compte aquestes infraestructures ja que el bloqueig o interrupció de determinats serveis (principalment *inalàmbrics*) podria venir també per les interferències que es poguessin

---

• La cuantía máxima de las sanciones pecuniarias que la Autoridad gubernativa esté autorizada para imponer, en su caso, a quienes contravengan las disposiciones que dicte durante el estado de excepción.".

El Congrés debatrà la sol·licitud d'autorització tramesa pel Govern i la pot aprovar "en sus propios términos o introducir modificaciones en la misma" (apartat 3).

Finalment, d'acord amb l'article 21 de la LOEE "la Autoridad gubernativa podrá suspender todo tipo de publicaciones, emisiones de radio y televisión, proyecciones cinematográficas y representaciones teatrales, siempre y cuando la autorización del Congreso comprenda la suspensión del artículo 20, apartados 1, a) y d), y 5 de la Constitución. Igualmente podrá ordenar el secuestro de publicaciones (apartat 1). Això no obstant, "el ejercicio de las potestades a que se refiere el apartado anterior no podrá llevar aparejado ningún tipo de censura previa" (apartat 2).

D'altra banda, l'apartat 4 de l'article 116 de la CE estableix que l'estat de setge serà declarat per la majoria absoluta del Congrés dels Diputats, a proposició exclusiva del Govern. El Congrés en determinarà l'àmbit territorial, la durada i les condicions.

D'acord amb l'article 32 de la LOEE, el Govern podrà proposar al Congrés dels Diputats la declaració de l'estat de setge "cuando se produzca o amenace producirse una insurrección o acto de fuerza contra la soberanía o independencia de España, su integridad territorial o el ordenamiento constitucional, que no pueda resolverse por otros medios" (apartat 1). Així mateix, "la correspondiente declaración determinará el ámbito territorial, duración y condiciones del estado de sitio" (apartat 2).

Finalment, l'apartat 3 de l'article 32 estableix que "la declaración podrá autorizar, además de lo previsto para los estados de alarma y excepción, la suspensión temporal de las garantías jurídicas del detenido que se reconocen en el apartado 3 del artículo 17 de la Constitución".

causar des d'aquestes infraestructures.

Seguint amb l'anàlisi de la normativa i d'aquest article 4 de la LGTEL cal fer esment també al seu apartat cinquè, que determina:

"*5. El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa de determinados servicios o de la explotación de ciertas redes de comunicaciones electrónicas, de acuerdo con el texto refundido de la Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto Legislativo 2/2000, de 16 de junio, para garantizar la seguridad pública y la defensa nacional*".

En relació amb aquesta previsió per tal de garantir la seguretat pública o bé la defensa nacional, el Govern de l'Estat espanyol pot acordar la gestió directa de determinats serveis de comunicacions electròniques o bé sotmetre'ls a les seves instruccions. Des d'aquesta perspectiva, les mesures tècniques a aplicar en aquest sector no són conegudes, malgrat que anirien alineades als objectius que es determinin; per exemple per al cas de la seguretat pública, s'inclouria l'ús de les infraestructures per difondre missatges d'emergència i per a la protecció de la població.

D'altra banda, la mateixa LGTEL també tracta aquesta possible imposició a través del servei públic definit a l'article 25. En particular el seu apartat primer determina que:

"*1. El Gobierno podrá, por necesidades de la defensa nacional, de la seguridad pública o de los servicios que afecten a la seguridad de las personas o a la protección civil, imponer otras obligaciones de servicio público distintas de las de servicio universal a los operadores*".

És aquest argument el que es podria fer servir per intervenir el funcionament normal dels serveis de les operadores de telecomunicacions. Deixant de banda les agressions externes a la sobirania que no correspondrien amb el cas d'estudi, cal recórrer a la Llei orgànica 4/1981, de l'estat d'excepció (LEE), on es regulen els estats d'alarma, excepció i setge. D'aquests tres, el que podria encaixar amb la situació que es planteja seria el de l'estat de setge que es defineix a l'article 32 de la LEE, com s'ha indicat anteriorment.

A mode de conclusió es pot afirmar, doncs, que el govern espanyol podria imposar mesures d'actuació excepcionals als operadors autoritzats a prestar serveis a nivell de l'Estat

espanyol, en l'etapa prèvia a la creació d'un Estat català. Sens perjudici d'això, és difícil determinar les mesures concretes que es podrien imposar ja que no n'hi ha precedents.

6. Els actius que cal protegir

En aquest apartat es descriuen i analitzen els diferents actius que podrien quedar afectats a conseqüència d'un mal funcionament dels sistemes de comunicacions electròniques.

Aquests actius, bàsics per a garantir el funcionament de l'eventual nou Estat català, es troben en els sectors de l'audiovisual, de les telecomunicacions i dels transports, i en l'àmbit dels serveis essencials.

A l'hora de triar els actius més importants es fa prevaler el criteri de dependència que tenen respecte de les comunicacions electròniques o sistemes d'informació.

6.1. El sector audiovisual

L'àmbit audiovisual està format per la transmissió del senyal de televisió i ràdio, des de la seva emissió en els diferents centres de producció audiovisual o radiofònica, fins a l'arribada als aparells de televisió o ràdio de les llars.

La televisió i la ràdio comparteixen la tecnologia mitjançant la qual es transporta el senyal des dels centres emissors fins als receptors finals.

6.1.1. La televisió i la ràdio

6.1.1.1. Descripció

La radiodifusió terrestre és el mètode tradicional de lliurament del senyal de TV i FM per ones de ràdio transmeses a través de l'espai obert. Els senyals són la TDT, l'FM i la DAB (tecnologia de ràdio digital actualment en proves).

A Catalunya, el punt principal de distribució del senyal de TDT, d'FM i de DAB, és la Torre de

Collserola (propietat de la Societat Torre de Collserola S.A. que té per objecte social la construcció i l'explotació del complex).

La Torre de Collserola rep el senyal de les diverses televisions (privades i públiques), l'empaqueta per a cada múltiplex (conjunt de canals) i el difon tant a l'Àrea Metropolitana com a la resta de centres emissors que conformen la xarxa de distribució del senyal, i als quals s'orienten les antenes de les llars per tal de rebre'l. De forma semblant actua la ràdio digital (DAB), per bé que actualment el servei es troba restringit a l'àmbit de la Torre de Collserola. En el cas del senyal d'FM, es distribueix de la mateixa forma fins a arribar al receptor (transistor domèstic, portàtil, de cotxe, etc.)

La Torre de Collserola (situada a l'Àrea Metropolitana, que concentra el 60% de la població total de Catalunya) distribueix els seus senyals, mitjançant radioenllaç i fibra òptica, als 8 centres reemissors principals de Catalunya. Entre tots permeten abastir el 85% de la població de Catalunya. Fins a arribar al 99,6% de la cobertura actual resten a la vora de 500 torres més que cobreixen la resta del territori i que distribueixen el senyal de TDT mitjançant radioenllaços i en algun cas via satèl·lit.

Pel que fa a la resta de tipologies de televisions (satèl·lit, cable i Internet) la seva penetració és inferior, però cal tenir-les presents.

- La televisió per satèl·lit, el senyal de la qual es lliura a les llars a través del transport via satèl·lit. Els satèl·lits d'Astra (19,2º est) –empresa luxemburguesa-, d'Eutelsat (Hot Bird 13º est) –empresa francesa- i d'Hispasat (30º oest) –empresa espanyola-, són els que principalment trameten canals en obert[4].
- El centre de control d'Abertis Telecom i de pujada del senyal als satèl·lits d'Hispasat està a les rodalies de Madrid. Però el senyal es pot pujar als satèl·lits d'Hispasat i també als d'Astra des de molts altres llocs del món.
- La televisió per cable és una forma de proveir el senyal de televisió directament a les llars mitjançant cable coaxial, parell de coure o fibra òptica. Cal dir que tots els aparells de TV que estan connectats al cable també poden veure la TDT i que la seva penetració és baixa.

[4] El centre de control d'Abertis Telecom i de pujada del senyal als satèl·lits d'Hispasat està a les rodalies de Madrid. Però el senyal es pot pujar als satèl·lits d'Hispasat i també als d'Astra des de molts altres llocs del món.

- La televisió per Internet tradueix els continguts en un format que pot ser transportat per ADSL, fibra òptica o altres tecnologies anomenades protocols d'Internet (Internet Protocol – IP). Per aquest motiu també es coneguda com a televisió IP. Actualment, encara no hi ha un alt grau de penetració d'aquests canals, no pas per una mancança tècnica dels receptors (televisors intel·ligents), sinó per la manca d'hàbit dels espectadors, que opten encara majoritàriament per l'oferta en TDT. Seria especialment interessant que les televisions catalanes estiguessin preparades per emetre a través d'Internet per tot el món.

6.1.1.2. El marc competencial

Sens perjudici de les competències atribuïdes a la Generalitat en els art. 137 i 140 de l'Estatut de Catalunya, l'espectre radioelèctric és un bé de domini públic, la titularitat, gestió, planificació, administració i control del qual és competència de l'Estat espanyol, d'acord amb la Constitució i l'article 43 de la Llei 32/2003, de 3 de novembre, general de telecomunicacions (LGTEL). Aquesta gestió s'exerceix de conformitat amb el que disposen el títol V de l'esmentada Llei i els tractats i acords internacionals dels quals Espanya n'és part, atenent la normativa aplicable de la Unió Europea (UE) i les resolucions i recomanacions de la Unió Internacional de Telecomunicacions (UIT) i d'altres organismes internacionals.

Així mateix, l'article 5 del Reglament de desenvolupament de la LGTEL, pel que fa a l'ús del domini públic radioelèctric, aprovat pel Reial decret 863/2008, de 23 de maig (Reglament LGTEL), estableix que "a fi d'aconseguir la utilització coordinada i eficaç del domini públic radioelèctric, el ministre d'Indústria, Turisme i Comerç, a proposta de l'Agència Estatal de Radiocomunicacions, ha d'aprovar el Quadre Nacional d'Atribució de Freqüències (CNAF) per als diferents tipus de serveis de radiocomunicació, d'acord amb les disposicions de la UE, de la Conferència Europea d'Administracions de Correus i Telecomunicacions (CEPT), i del Reglament de radiocomunicacions de la UIT, i definir l'atribució de bandes, subbandes, freqüències, canals i els circuits radioelèctrics corresponents, així com les altres característiques tècniques que puguin ser necessàries."

Mitjançant l'Ordre IET/787/2013, de 25 d'abril, el Ministeri d'Indústria, Energia i Turisme va aprovar el CNAF, que, pel que fa als serveis de comunicació audiovisual (radiodifusió sonora i televisió), estableix unes bandes de freqüències tot remetent-se als corresponents plans

tècnics nacionals, l'elaboració dels quals és una facultat assignada al Govern de l'Estat en relació amb la gestió del domini públic radioelèctric, d'acord amb l'article 44 de la LGTEL.

En definitiva, els serveis de comunicació audiovisual es transmeten dins de les bandes de freqüències que s'assignen internacionalment per a aquesta finalitat i, posteriorment, l'Estat espanyol defineix l'atribució de bandes, subbandes, freqüències, canals i els circuits radioelèctrics corresponents, així com les altres característiques tècniques que puguin ser necessàries, mitjançant el CNAF i, en determinats supòsits, tenint en compte els corresponents plans tècnics nacionals que, pel que fa a la ràdio i la televisió, són els següents:

- El Pla Tècnic Nacional de Radiodifusió Sonora en Ones Mitjanes (hectomètriques), aprovat pel Reial decret 765/1993, de 21 de maig, i modificat per la Resolució de 23 d'abril de 2002[5].
- El Pla Tècnic Nacional de Radiodifusió Sonora Digital Terrestre aprovat pel Reial decret 1287/1999, de 23 de juliol, modificat pels Reials decrets 776/2006, de 23 de juny, i 802/2011, de 10 de juny, i complementat per les ordres de 23 de juliol de 1999, de 24 d'agost de 1999, de 15 d'octubre de 2001 i de 13 de juliol de 2011[6].
- El Pla Tècnic Nacional de la Televisió Digital Terrestre aprovat pel Reial decret 944/2005, de 29 de juliol, modificat pels reials decrets 920/2006, de 28 de juliol, i 365/2010, de 26 de març, i complementat per l'Ordre ITC/2212/2007, de 12 de juliol.

[5] La nota d'utilització UN-1 del CNAF estableix que la banda de freqüències 526,5 a 1606,5 kHz s'utilitzarà exclusivament per les entitats habilitades per a la prestació dels serveis de radiodifusió sonora en ona mitjana. Aquestes entitats habilitades són: la Corporació de Ràdio i Televisió Espanyola, S.A., a través de la Sociedad Mercantil Estatal Ràdio Nacional d'Espanya (RNE) i les persones físiques o jurídiques mitjançant el títol habilitant atorgat per l'Estat per a l'explotació en gestió indirecta.

[6] La nota d'utilització UN-96 del CNAF estableix que la banda de freqüències 195 a 223 MHz s'utilitzarà exclusivament per les entitats habilitades per a la prestació dels serveis de radiodifusió sonora digital terrestre. Aquestes entitats habilitades són: la Corporació de Ràdio i Televisió Espanyola, S.A., a través de la Sociedad Mercantil Estatal RNE; les persones físiques o jurídiques mitjançant títol habilitant atorgat per l'Estat per a l'explotació en gestió indirecta en les xarxes de cobertura estatal; els ens públics amb competència en la matèria de les comunitats autònomes; les persones físiques o jurídiques mitjançant concessió administrativa atorgada pels òrgans competents de les comunitats autònomes per a l'explotació en gestió indirecta en les xarxes de cobertura territorial autonòmica; les persones físiques o jurídiques mitjançant concessió administrativa atorgada pels òrgans competents de les comunitats autònomes per a l'explotació en gestió indirecta en una demarcació de cobertura local.

- El Pla Tècnic Nacional de la Televisió Digital Local, aprovat pel Reial decret 439/2004, de 12 de març, modificat pels Reials decrets 2268/2004, de 3 de desembre, i 944/2005, de 29 de juliol, i complementat per l'Ordre de 30 de desembre de 2004[7].
- El Pla Tècnic Nacional de Radiodifusió Sonora en Ones Mètriques amb Modulació de Freqüència, aprovat pel Reial decret 964/2006, d'1 de setembre[8].

6.1.1.3. Escenaris de col·laboració i riscos

Com ja s'ha dit, d'acord amb la normativa vigent, l'espai radioelèctric és un bé de domini públic estatal i, en conseqüència, en la transició cap al nou Estat, l'escenari desitjable és el de col·laboració amb el govern espanyol, per tal de fer el traspàs de les competències i freqüències radioelèctriques, així com de les llicències habilitants dels operadors audiovisuals i els drets i deures econòmics associats.

En el cas de no existir una voluntat de col·laboració, l'Estat espanyol podria interferir tècnicament la difusió audiovisual, de tal manera que dificultés l'emissió de continguts. Això seria factible a través d'Abertis Telecom, el qual disposa de l'adjudicació de transport i

[7] Les notes d'utilització UN-35 i UN-36 del CNAF estableixen que la banda de freqüències 470 a 862 MHz (canals radioelèctrics 21 a 69) s'utilitzarà per les entitats habilitades per a la prestació dels serveis de televisió amb tecnologia digital. Aquestes entitats habilitades són: la Corporació de Ràdio i Televisió Espanyola, S.A., mitjançant la Sociedad Mercantil Estatal Televisión Española (TVE); les societats anònimes mitjançant títol habilitant atorgat per l'Estat per a l'explotació en gestió indirecta en una xarxa de cobertura estatal -Antena 3 de Televisión, S.A. (A3), Sogecable, S.A. (C4), Gestevisión-Telecinco, S.A. (T5), Gestora de Inversiones Audiovisuales La Sexta (L6), Gestora de Televisión Net TV, S.A. i Veo Televisión, S.A.-; els ens públics amb competència en la matèria de les comunitats autònomes que han obtingut el títol habilitant per a la gestió directa de la televisió en un múltiple digital d'àmbit territorial autonòmic; les persones físiques o jurídiques mitjançant títol habilitant atorgat pels òrgans competents de les comunitats autònomes per a l'explotació en gestió indirecta en un múltiple digital de cobertura territorial autonòmica; els municipis i les organitzacions territorials insulars mitjançant títol habilitant atorgat pels òrgans competents de les comunitats autònomes per a l'explotació en gestió indirecta en una demarcació de cobertura local; les persones físiques o jurídiques mitjançant títol habilitant atorgat pels òrgans competents de les comunitats autònomes per a l'explotació en gestió indirecta en una demarcació de cobertura local.

[8] La nota d'utilització UN-17 del CNAF estableix que la banda de freqüències 87,5 a 108 MHz s'utilitzarà exclusivament per les entitats habilitades per a la prestació dels serveis de radiodifusió sonora en ones mètriques amb modulació de freqüència. Aquestes entitats habilitades són: la Corporació de Ràdio i Televisió Espanyola, S.A., mitjançant la Sociedad Mercantil Estatal Radio Nacional de España (RNE); els ens públics amb competència en la matèria de les comunitats autònomes (emissores FM autonòmiques); les Corporacions Locals mitjançant títol habilitant atorgat pels òrgans competents de les comunitats autònomes (emissores FM municipals); les persones físiques o jurídiques mitjançant títol habilitant atorgat pels òrgans competents de les comunitats autònomes, o en el seu cas per l'Estat, per a l'explotació en gestió indirecta.

difusió del senyals audiovisuals, en aquells canals de TDT o ràdio que utilitzen les cadenes públiques i privades de Catalunya.

Es podrien produir interferències electròniques en les bandes utilitzades per a la difusió de la TDT i l'FM, ja siguin induïdes mitjançant antenes mòbils desplegades o mitjançant avions especialitzats que són capaços de generar interferències sota l'espai que sobrevolen.

6.1.1.4. Alternatives

Per garantir l'emissió de la TDT, el primer que s'ha d'assegurar és la generació de continguts i senyals, a continuació el transport d'aquest senyal al centre emissor i finalment la difusió d'aquest senyal a la població. En aquest sentit, cal disposar d'alternatives. A Catalunya tenim la possibilitat de duplicar tant la generació de continguts i senyal, com el transport i fins i tot la difusió. Per a la generació de continguts i elaboració del senyal hi ha empreses que actualment ja realitzen aquestes activitats per a les seves pròpies necessitats o per als seus clients. També existeixen alternatives en el transport del senyal amb fibra i ràdio fins a Collserola: la Generalitat té fibres que arriben a Collserola i que connecten TVC , CatRadio i els principals punts de la ciutat de Barcelona.

En teoria, una altra alternativa seria executar el pla de recuperació de desastres, consistent a duplicar, amb instal·lacions alternatives, els centres de control i emissió de radiofreqüència. Tanmateix, cal reconèixer que la inversió econòmica que requeriria aquest pla de recuperació en les circumstàncies actuals el fa poc viable a la pràctica.

En tot cas, davant d'una "interferència" estatal pel que fa a l'emissió dels canals de TDT i FM públics i privats de Catalunya, caldria tenir en compte que:

- Tot i que l'espai radioelèctric és un bé de domini públic estatal, Catalunya, atès que atorga els títols habilitants, pot gestionar aquella part que s'ubica sobre el seu territori.
- Els prestadors de serveis de comunicació audiovisual catalans tenen el dret a prestar el servei i, en conseqüència, tenen també el dret d'accés a les xarxes electròniques per poder-lo prestar.
- Els serveis de comunicació audiovisual radiofònics, televisius i connexos i interactius són serveis d'interès general que es presten en l'exercici del dret a la

lliure expressió d'idees, del dret a comunicar i rebre informació. Aquests drets tenen reconeixement i protecció constitucional.

- La pròpia normativa estatal atorga al servei de comunicació audiovisual públic la condició de servei essencial d'interès econòmic general.

Finalment, en relació amb els prestadors de serveis de comunicació audiovisuals estatals que emeten a Catalunya, el Govern de la Generalitat hauria de seguir mantenint la situació actual pel que fa als prestadors privats mitjançant un acord amb Abertis Telecom i, d'altra banda, mitjançant la signatura d'un acord transfronterer amb l'Estat espanyol pel que fa a l'emissió dels prestadors públics.

Així mateix, en aquest context, el CTTI[9] -empresa pública creada per llei el 28 de desembre de 1993, i adscrita al Departament d'Empresa i Ocupació- seria l'encarregada de vetllar per l'estricte compliment de les obligacions que Abertis Telecom té assumides en virtut del Contracte d'Arrendament d'Infraestructures (CAI) i dels contractes de prestació de serveis de transport i difusió dels senyals televisius i radiofònics de la Corporació Catalana de Mitjans Audiovisuals i, en definitiva, del manteniment dels serveis públics de comunicació audiovisual.

Analitzades les estratègies i mesures per fer front a situacions de risc, cal analitzar també les estratègies i mesures que hauria d'adoptar el nou Estat per tal de poder exercir les competències que avui exerceix l'Estat espanyol. En efecte, en el supòsit que Catalunya esdevingués un estat independent, per tal d'elaborar el seu propi CNAF, hauria de sol·licitar l'adhesió a l'UIT. Aleshores, com a Estat membre de l'UIT, podria definir l'atribució de bandes, subbandes, freqüències, canals i els circuits radioelèctrics corresponents, així com les altres característiques tècniques que poguessin ser necessàries.

Així mateix, i de manera paral·lela, la Generalitat hauria de regular el domini públic radioelèctric (l'espectre radioelèctric), el domini públic de numeració (els números assignats a la telefonia), el segment espacial (òrbites dels satèl·lits) i el domini públic radioelèctric

[9] El Govern de la Generalitat va constituir el Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) per integrar tots els serveis informàtics i de telecomunicacions de l'Administració en una única estructura. Per tant, el CTTI és el responsable de garantir la direcció, planificació, gestió i control dels sistemes d'informació i dels serveis de telecomunicacions de la Generalitat de Catalunya. Alhora dissenya, construeix, coordina i desplega els projectes que la Generalitat li encarrega per desenvolupar i fer créixer la Societat del Coneixement.

terra-espai (enllaços ascendents i descendents entre les estacions terrestres i els satèl·lits), tot assumint-ne la titularitat, la gestió, la planificació, l'administració i el control. Això comportaria que Catalunya podria crear xarxes de comunicacions electròniques pròpies[10]. En aquest sentit, es podria analitzar la conveniència o no de crear una entitat pública específicament encarregada de gestionar directament la xarxa i prestar serveis de transport i de difusió del senyal audiovisual o, en el seu cas, de fer-ho mitjançant la gestió indirecta a través d'una entitat privada, prèvia la corresponent concessió administrativa.

6.2. El sector de les telecomunicacions

Realitzar una trucada telefònica des de casa mitjançant el mòbil, consultar el correu electrònic, etcètera, són serveis de telecomunicacions que se suporten en xarxes. Les xarxes de telecomunicacions es componen de nodes (equips electrònics situats dins d'edificis especialitzats) i connexions entre nodes. Són usualment sistemes de transmissió de senyals basats en fibra òptica, que connecten els edificis. Els clients finals es connecten als nodes mitjançant cable de coure o fibra òptica des de les llars, o també mitjançant ones electromagnètiques que permeten la connexió a les antenes de telefonia mòbil (aquestes antenes, estacions base en l'argot del sector, es connecten amb els nodes).

Les xarxes públiques que donen actualment servei a Catalunya formen part de xarxes d'abast estatal, gestionades i operades des de centres de gestió situats majoritàriament a Madrid. Aquests centres de gestió poden desconnectar nodes de la xarxa, desconnectar antenes, deixar fora de servei els clients dins d'un node, tallar les interconnexions entre nodes de manera total o parcial. Podríem dir que la xarxa és "esclava" del centre de gestió. Aquesta situació és important per tal d'avaluar correctament la situació.

[10] Xarxa de comunicacions electròniques. Sistemes de transmissió i, si escau, els equips de commutació o encaminament i d'altres recursos que permetin el transport de senyals mitjançant cables, ones hertzianes, mitjans òptics o d'altres mitjans electromagnètics amb inclusió de les xarxes de satèl·lits, xarxes terrestres fixes i mòbils, sistemes de tendals elèctrics, 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.

6.2.1. La telefonia fixa i mòbil (veu)

6.2.1.1. Descripció

La telefonia, tant la fixa com la mòbil, es basa en l'ús del sistema de numeració, que integra uns dels dominis públics del camp de les telecomunicacions.

Aquest sistema de numeració té un prefix identificatiu de l'Estat, el qual és assignat per la ITU (Unió Internacional de Telecomunicacions) –a Espanya, com és conegut, li correspon el número 34- i un conjunt de números que identifiquen l'emissor de la trucada i el receptor. L'encaminament d'aquesta trucada fins al seu receptor requereix unes tecnologies i acords d'intercanvi d'aquestes trucades entre operadors de telecomunicacions dels diferents països, que estan regulats internacionalment. No són aliens a aquesta problemàtica els números especials, com per exemple emergències (112) o informació de l'Administració (010 o 012). L'Estat és el titular del domini públic de numeració i n'atorga l'ús a les empreses autoritzades a prestar el servei de telefonia.

Pel que fa a la veu, a la xarxa de telefonia mòbil es transmet a través d'una xarxa d'estacions base, interconnectades per xarxes de fibra òptica o per radioenllaços, propietat dels operadors autoritzats (Telefónica, Orange, Vodafone i Yoigo), els quals reben i emeten les trucades dels telèfons mòbils que es troben en el seu abast, a través de l'emissió d'ones a una determinada freqüència assignada per l'Estat, ja que és l'ens competent.

Tanmateix, l'evolució de la tecnologia de telefonia mòbil fins a l'actual 3G o 4G també permet la connexió a Internet (transmissió de dades).

6.2.1.2. Marc competencial

La liberalització de les comunicacions telefòniques suposa que aquestes funcionin en tant que les operadores funcionin. Aquestes operadores segueixen les regulacions internacionals que marca la Unió Internacional de Telecomunicacions. Per tant, la Generalitat no té cap competència sobre la telefonia. Però l'Estat tampoc no té potestat per fer que els telèfons deixin de funcionar.

6.2.1.3. Escenaris de col·laboració i riscos

Durant el procés de Transició Nacional caldria acordar amb l'Estat espanyol el manteniment del prefix estatal +34 fins que l'eventual Estat català esdevingués membre de la ITU, la qual hauria d'atorgar un nou prefix internacional per al territori de Catalunya. Un entorn de col·laboració amb l'Estat espanyol donaria seguretat a les operadores.

De fet, no existeix cap instrument legal que permeti que l'Estat pugui forçar les operadores a suspendre els serveis de telefonia. Les operadores importants, que poden mantenir el sistema de comunicacions telefòniques, són internacionals i cotitzen a Borsa. Amb tota seguretat la pressió de l'Estat espanyol sobre aquest tipus d'empreses seria infructuosa. Per tant, es pot considerar poc probable que es materialitzi el principal risc identificat, que seria no poder establir l'encaminament de les trucades en general, però especialment als serveis d'emergències o institucionals (112, 061, 080, 010, 012...).

Com en altres casos, tampoc aquí no existeixen mecanismes jurídics per poder impedir el funcionament d'alguns punts d'interconnexió de les operadores, llevat del cas que es declarés un estat d'excepció. Altra cosa és que es puguin produir accions de sabotatge. També cal tenir en compte els interessos privats que interactuen en aquest àmbit, que depenen dels seus accionistes i no de les instruccions de l'Administració estatal.

En el cas de la telefonia mòbil, igual que en el de la TDT i ràdio, també ens podríem trobar amb interferències electròniques en les freqüències utilitzades per les operadores de telefonia mòbil, induïdes mitjançant antenes mòbils desplegades o mitjançant els avions especialitzats en els atacs electrònics, capaços de generar interferències sota l'espai que sobrevolen. Tanmateix, l'acció d'aquesta mena d'avions només pot acotar-se a espais limitats, de manera que no esdevé un risc real, si no és que es focalitzi sobre espais especialment rellevants.

Un dels riscos que cal tenir en compte és la inestabilitat en les comunicacions que eventualment es podria produir arran de sabotatges a la xarxa, provocant caigudes de nodes territorials, numeracions selectives o d'altres.

Fins i tot es podrien impedir totes les comunicacions, tret de l'accés al 112. Intentar impedir aquestes accions és força complicat i exigiria desendollar els nodes dels sistemes de gestió i la capacitat d'operar localment. Malgrat aquesta situació, les xarxes de titularitat de la

Generalitat podrien reconfigurar-se i mantenir-se actives.

Aquesta situació d'excepcionalitat només es podria mantenir durant un període de temps curt, atesa l'afectació a les persones i empreses. Per això seria necessari un estudi en profunditat de les alternatives d'emergència basades en xarxes pròpies i serveis internacionals.

És important assenyalar que per donar continuïtat al servei, tant de la xarxa fixa com de la mòbil, és necessari disposar de fibra òptica i d'interconnexió amb els operadors situats a Catalunya o a fora de Catalunya.

Els terminals via satèl·lit, especialment serveis basats en operadors internacionals com Inmarsat, es podrien veure afectats per interferències generades localment, és a dir, a prop dels terminals.

6.2.1.4. Alternatives

En el cas de la telefonia, no caldrien actuacions específiques, ja que les operadores en garantirien el funcionament.

El que sí que caldrà fer, en cas que Catalunya esdevingui un nou Estat, és integrar-se a la ITU i demanar un codi de país per a les trucades internacionals. En aquest sentit, caldria que el Govern establís relacions amb la ITU al més aviat possible.

6.2.2. Internet

Internet és una xarxa pública i global d'ordinadors interconnectats mitjançant el protocol d'Internet (IP) i que envien les dades de l'emissor al receptor i viceversa. Internet és la unió de moltes altres xarxes, ja siguin acadèmiques, comercials o de les administracions. Per tant, caldria prestar especial cura a l'hora de determinar el possible impacte d'un tall d'aquest servei.

L'accés a les xarxes de dades, majoritàriament Internet, es fa mitjançant els parells de coure o cables de fibra òptica que connecten els edificis dels clients, llars o empreses, o des dels terminals mòbils tipus *smartphone* o enrutaments habilitats per connexions de ràdio.

Malgrat que són xarxes diferents de les esmentades en l'apartat de telefonia, comparteixen el primer tram, coure/fibra o connexió terminal-antena. Això implica que els propietaris d'aquest primer tram en controlen l'accés.

El mercat d'Internet està compost per diferents proveïdors (*Internet Service Providers*, ISP) i està més atomitzat que el dels serveis de telefonia. Tot i això, la majoria de clients pertanyen als grans operadors (Telefònica, Vodafone, Orange…). Els operadors alternatius no disposen de xarxes pròpies per interconnectar-se amb el nodes d'intercanvi i fan servir les infraestructures (fibra òptica) dels grans operadors.

A Catalunya hi ha algunes infraestructures específiques, que les diverses xarxes existents (acadèmiques, comercials, de l'administració, privades, etc.) utilitzen per intercanviar-se la informació, que garanteixen que l'emissor i el receptor es connectin i comuniquin. Si aquests punts, pel motiu que sigui, deixen de fer aquesta funció, el tràfic es talla i els serveis es deixen de prestar. Són el que anomenem nusos de connexió.

La connexió a Internet es produeix, per tant, des de i cap a un proveïdor d'Internet que està connectat a un d'aquests nusos de comunicacions. Les diferents tecnologies que permeten la connexió entre el nostre dispositiu (fix o mòbil) amb el proveïdor d'Internet són les següents: fibra òptica, ADSL (parell de coure), Internet mòbil (EDGE, 3G, 4G), WiMAX i connexió per satèl·lit. A continuació fem una breu descripció de cadascuna.

- Fibra òptica

La fibra òptica és la principal tecnologia per a la connexió a Internet, ja que la seva alta capacitat permet altres formes de connexió (3G, 4G, WiMAX).

Ara per ara l'extensió del cable i fibra òptica pel territori fa difícil el sabotatge o la tallada massiva de cables. Tot i així, cal garantir la integritat física d'alguns punts estratègics, ja siguin nusos de comunicació o punts únics de sortida i/o entrada de les telecomunicacions.

- Internet mòbil (EDGE, 3G, 4G)

L'evolució de la tecnologia de telefonia mòbil fins a l'actual 3G o 4G permet la connexió a Internet (dades) d'uns telèfons cada cop més potents i amb incomptables aplicacions.

Per aquest motiu els operadors de telefonia mòbil interconnecten les seves antenes amb

xarxes de fibra òptica per tal de garantir una velocitat d'intercanvi d'informació major que si s'utilitzessin ones convencionals. En aquest cas és molt important garantir que els dispositius mòbils disposin de connexió. Per posar en relleu la seva importància, n'hi ha prou de recordar el paper que han tingut en les denominades primaveres àrabs.

- ADSL

L'ADSL és la tecnologia emprada per fer arribar Internet mitjançant els cables de coure que utilitza la telefonia fixa.

- WiMAX

En aquells indrets de major dificultat d'accés, tot i arribar-hi la telefonia fixa, no és possible accedir a Internet amb el cablejat de parell de coure, per la qual cosa la connexió a Internet arriba mitjançant el que s'anomena WiMAX. Aquesta tecnologia utilitza les ones per fer arribar la connexió des d'una antena emissora fins a les antenes receptores de les llars, les quals són capaces de descodificar el senyal. Les antenes de WiMAX, solen estar connectades a xarxes de fibra òptica, com en el cas de les antenes de telefonia mòbil.

- Connexió per satèl·lit

El darrer tipus de connexió a Internet que s'utilitza, tot i que en menor grau, és la connexió per satèl·lit. Mitjançant una antena parabòlica, el proveïdor d'Internet fa arribar la connexió a través del satèl·lit.

- Els nusos de comunicacions

Els nusos de comunicacions, com ja s'ha dit anteriorment, són els punts on s'intercanvien la informació de les diferents xarxes i proveïdors d'Internet. Es poden associar amb la idea de les portes de sortida cap a Internet. Els proveïdors d'Internet intercanvien dades als NAP (*Network Access Points*). Als més importants només hi accedeixen els gran operadors a escala global, com Vodafone, ATT, Verizon, Telefónica, Orange i altres d'aquest nivell. El principal de l'Estat Espanyol és l'HISPANIX, que és a Madrid.

La Generalitat disposa del CATNIX, el nus de comunicacions neutre que està situat a la Universitat Politècnica de Catalunya (UPC) i on s'intercanvien el tràfic de dades les diverses operadores. S'hauria de dimensionar el CATNIX per suportar el tràfic amb origen i destinació

Catalunya.

6.2.2.1. Riscos

Els nusos de comunicació estan connectats a Internet sense cap jerarquia establerta i, en la seva majoria, estan en mans d'empreses privades. Això garanteix, com en el cas de la telefonia, que tot i que algun nus de comunicació pogués deixar de donar servei per sabotatge, Catalunya no deixaria d'estar connectada a Internet. Es podrien produir col·lapses o lentitud de la xarxa de forma local, però de forma legal no es pot desconnectar tot Catalunya d'Internet.

Ara bé, al marge de la legalitat es podrien produir sabotatges, apagades d'equips electrònics o atacs informàtics que podrien generar algunes situacions puntuals de col·lapse de la xarxa d'Internet a Catalunya.

Com en el cas de la telefonia, els centres de gestió podrien desconnectar totalment o parcialment les xarxes. La majoria d'operadors alternatius fan servir els ADSL de Telefónica, els quals depenen del seu sistema de gestió.

En definitiva, en aquest àmbit seria necessari establir els mateixos escenaris de col·laboració amb l'Estat espanyol que en el cas de xarxes de telefonia, de cara a garantir l'estabilitat dels agents i els operadors. Però cal ser conscients que, en un entorn de desacord, també es produirien els mateixos riscos que en el cas de xarxes de telefonia. Això no obstant, la major diversificació d'operadors i proveïdors de fibra, fins i tot les fibres òptiques de la xarxa pròpia de la Generalitat, permetrien una sortida a Internet. Aquestes fibres haurien de protegir-se d'eventuals talls provocats en el seu recorregut o en els edificis de concentració i de pas.

També es podria considerar el risc de censura, tal com existeix, per exemple, a la Xina. Però cal tenir en compte que a tota la UE, les telecomunicacions estan liberalitzades, i seria molt difícil implantar un sistema de censura a la xarxa.

6.2.2.2. Alternatives

La situació de contingència per garantir la connectivitat a Internet passa per tenir prevista la possibilitat de fer circular el tràfic d'Internet de tot Catalunya a través del CATNIX, el punt

neutre de connexió a Internet de la Generalitat de Catalunya.

Actualment totes les operadores tenen algun enrutament de tràfic a través del CATNIX. És fonamental, doncs, que Telefónica, com a principal proveïdor de serveis d'Internet a Catalunya, s'afegeixi a aquest nus de comunicació neutre

L'accés a Internet via satèl·lit no té les mateixes capacitats que la fibra òptica però és una alternativa a considerar, especialment per distribuir continguts a servidors d'arreu del món. Per accedir als satèl·lits existeixen equips mòbils de desplegament ràpid (*fly away*) que són difícilment interceptables. Només es podria plantejar dur a terme la connexió a Internet de forma massiva, per tecnologia satèl·lit, a través de l'estació de la Granada del Penedès, però a causa del seu estat d'abandonament, avui en dia no seria viable.

A banda dels riscos i les seves alternatives, durant el procés de Transició Nacional, l'eventual constitució d'un Estat català també exigiria prendre altres decisions de relleu. Per exemple, i igualment en el cas de les xarxes fixes i mòbils, caldria fer la separació de la xarxa d'àmbit català i la implementació dels seus sistemes propis de gestió i operació. L'intercanvi de dades entre operadors s'hauria de fer al CATNIX.

A diferència de la telefonia, la numeració, és a dir, les adreces IP, és més flexible i el període transitori estaria més lligat al pas del domini .es (webs amb adreça acabada en .es (Espanya) a .cat (Catalunya)). Recordem que Catalunya, malgrat no ser un Estat, ja va aconseguir fa uns quants anys un domini propi.

Caldria garantir la sortida a Internet i, per tant, caldria tenir capacitat i fibra al CATNIX i als punts d'intercanvi de tràfic alternatius a Barcelona. També caldria garantir que aquests punts d'intercanvi estiguessin connectats al món a través d'interconnexions internacionals amb fibra o satèl·lit com a últim recurs.

6.2.3. Xarxa RESCAT

6.2.3.1. Descripció

La Xarxa RESCAT és la xarxa de telecomunicacions que utilitzen el cos de Mossos d'Esquadra, les policies locals i alguns dels cossos d'emergència de Catalunya (SEM,

agents rurals, bombers). La xarxa està sostinguda per una infraestructura de titularitat pública, operada per l'empresa privada Abertis Telecom.

6.2.3.2. Marc competencial

La Xarxa RESCAT opera sobre unes freqüències atorgades per l'Estat a la Generalitat de Catalunya. És aquesta qui estableix la concessió de la gestió de la xarxa a l'operadora Abertis per tal que ofereixi el servei. És a dir, la Generalitat és el client i, per tant, qui paga a Abertis per mantenir el servei de la Xarxa RESCAT.

6.2.3.3. Escenari de col·laboració i riscos

L'escenari de col·laboració en aquest apartat està restringit al traspàs de la titularitat de la freqüència que utilitza la xarxa RESCAT a l'Administració catalana, que ja gestiona l'esmentada freqüència.

En un escenari de no-col·laboració, i igual que en altres apartats anteriors, es podrien produir interferències electròniques en les bandes utilitzades per la Xarxa RESCAT, ja sigui mitjançant antenes o mitjançant uns avions especialitzats en atacs electrònics capaços de generar interferències sota l'espai que sobrevolen.

També es podria considerar, per bé que remotament, la retirada de l'autorització de l'Estat per a l'ús de les freqüències, amb la generació de la necessitat que el futur Govern de la Generalitat aprovés novament aquesta autorització en ús de les capacitats que li proporcionaria succeir l'Estat en aquest àmbit.

Cal tenir present que RESCAT fa servir freqüències compartides amb la policia nacional espanyola i que aquesta té una xarxa paral·lela a RESCAT activa i funcionant a Catalunya. Per tant, si la policia espanyola activa la seva xarxa amb noves freqüències i més potència que RESCAT, podria provocar seriosos problemes per funcionar, sobretot a la ciutat de Barcelona.

6.2.3.4. Alternatives

De la mateixa manera que amb els serveis audiovisuals, les alternatives per garantir la Xarxa RESCAT passarien per tenir el control operatiu de la Torre de Collserola i els repetidors

principals al territori.

El col·lectiu de radioaficionats es podria considerar una altra xarxa especial. Els radioaficionats són un conjunt d'usuaris degudament autoritzats, que utilitzen diversos tipus d'equips de radiocomunicació per a comunicar-se amb altres radioaficionats d'arreu del món per al servei públic, la recreació i la formació.

6.3. El sector del transport

Aquest sector és altament dependent de les comunicacions electròniques. En aquests casos parlem sobretot de les instal·lacions radioelèctriques d'ajuda a la navegació aèria, marítima o ferroviària. El transport per carretera, tot i no tenir aquesta dependència per a la navegació, si que es podria veure afectat per una pèrdua d'informació sobre les comandes, compres, destins de mercaderies, etc.

6.3.1. El transport aeri

6.3.1.1. Descripció d'infraestructures clau

El transport aeri es recolza en instal·lacions radioelèctriques d'ajuda a la navegació. Existeixen determinades instal·lacions que tenen constituïdes servituds radioelèctriques per assegurar l'adequat funcionament de les estacions que garanteixen la comunicació entre els avions i la torre de control o entre els mateixos aparells.

A Catalunya, els aeroports tenen una torre que controla l'enlairament i l'aterratge dels avions a les dependències aeroportuàries, però també existeix el Centre de Control de Barcelona, seu de la Direcció Regional de Navegació Aèria Est, una instal·lació de vital importància per a la navegació aèria. Aquest centre controla el trànsit i aproximació als aeroports del territori que li és assignat.

6.3.1.2. Marc competencial

En l'àmbit de les comunicacions electròniques que s'utilitzen per a la gestió de l'espai aeri, l'Estat té totes les competències. Estan regulades pel Reial decret 57/2002, de 18 de gener,

pel qual s'aprova el Reglament de circulació aèria. La normativa de circulació aèria incorporada a aquest Reial decret no és més que l'adaptació a l'ordenament espanyol de les modificacions que l'Organització d'Aviació Civil Internacional (OACI) ha anat introduint en el Conveni de Chicago.

6.3.1.3. Riscos

En aquest cas seria molt important la col·laboració amb l'Estat per poder dur a terme un traspàs ordenat i segur de la gestió de les freqüències i els centres de control, atesa la rellevància que tenen les comunicacions per a la seguretat en la navegació aèria. Seria també convenient establir acords de col·laboració amb els altres estats limítrofs.

El principal risc és el tancament de l'espai aeri només sobre Catalunya i la paralització consegüent de l'aeroport del Prat. Existeixen alternatives tècniques per suplir aquesta mancança, en el supòsit que el Govern ho considerés necessari. En cas contrari, només amb el control físic de la instal·lació se'n podria garantir el funcionament. Cal dir, però, que seria altament improbable que l'Estat tanqués l'espai aeri sobre Catalunya, ja que estaria incomplint les normatives d'aviació civil internacional i creant un caos a nivell continental, tal com va passar el 2009 amb la vaga de controladors. En aquest sentit, cal tenir en compte el fet diferencial que un Estat no pot tancar l'espai aeri unilateralment sense provocar una reacció internacional.

6.3.1.4. Antecedents

En els recents processos d'independència hi ha exemples de casos de canvi de sobirania sobre un determinat espai aeri que han provocat seriosos conflictes, però també n'hi ha d'altres en els quals el traspàs de sobirania a les noves autoritats es va produir de manera pacífica i pactada.

El traspàs de control de comunicacions equival al traspàs del control de la infraestructura, i en el cas de Catalunya el seu èxit dependria de com es negociï el traspàs de l'Estat espanyol (avui d'Aena) al nou Estat català de la gestió de control de l'espai aeri català.

Durant aquest traspàs cal tenir en compte que el control de l'espai aeri dependria, tant durant les fases de vol com d'aproximació, del centre de control, mentre que en l'enlairament o l'aterratge ho faria només dels sistemes del propi aeroport.

6.3.2. El transport marítim

6.3.2.1. Descripció

Bàsicament els sistemes de radiocomunicacions marítimes estan orientats a la comunicació entre vaixells i els ports i al rescat. Conviuen junts els sistemes civils i els militars, que per la seva naturalesa, són xifrats.

Els equips que ofereixen aquests serveis són els següents:

- Ràdio i Navtex (amb les bandes de freqüència en MF, HF i VHF) (Radiotelègraf);
- Satèl·lit (COSPAS-SARSAT, balises, Inmarsat);
- Transponedors de radar

En ser elements de seguretat de la vida humana i del tràfic marítim nacional i internacional, i pel fet que Catalunya es troba en un indret geogràfic estratègicament clau en el pas de vaixells per la Mediterrània, així com un centre de distribució logística per a Espanya i Europa, és poc probable la seva interferència. Cal remarcar que les interferències en les comunicacions via satèl·lit són pràcticament impossibles.

A priori totes les comunicacions són secretes i està totalment prohibida la divulgació o utilització del contingut sense l'exprés consentiment de l'emissor. Qualsevol persona que escolti els missatges emesos i no en sigui el destinatari té l'obligació de guardar el secret dels seus continguts. En les comunicacions marítimes totes les comunicacions són en obert, és a dir, no estan encriptades. Tant l'emissor com el receptor tenen l'obligació d'identificar-se verbalment o digitalment. Les comunicacions de seguretat o emergència tenen prioritat sobre totes les altres.

- NAVTEX

És un sistema per transmetre i rebre informació de text: avisos de navegació, meteorològics, urgència o seguretat, a través de la impressió telegràfica de banda estreta. Aquestes informacions es transmeten des de les estacions base costaneres a equips específics embarcats en els vaixells. El NAVTEX està pensat per difondre aquesta informació dins els límits de les aigües costaneres (400 milles -740 km).

- Sistemes de satèl·lits
    - INMARSAT

Es tracta d'un sistema de satèl·lits, el propòsit del qual és proporcionar l'espai per a les comunicacions marítimes via satèl·lit amb l'objectiu de millorar les comunicacions d'auxili i seguretat de la vida humana al mar, la gestió dels vaixells, els serveis de correspondència pública i els de radiolocalització. Inmarsat està dividit en dues societats: una de pública, destinada als sistemes d'auxili, i una de privada, que ofereix sistemes de telecomunicacions a tot el globus terraqüi. El sistema està compost per 4 satèl·lits en òrbita geostacionària a 36.000 km orbitant en l'equador i al voltant de la Terra, amb 4 satèl·lits de reserva i ofereix cobertura entre els 70º N i els 70º S. Existeixen altres sistemes de comunicació per satèl·lit, com el GLONASS, que orbita zenitalment i ofereix cobertura en els pols Nord i Sud.

    - COSPAS-SARSAT

El seu significat és *Cospas*: *Space System for Search and Distress Vessels – Sarsat: Search and Rescue Satelite-Aided*.

És un sistema de satèl·lit dissenyat per localitzar radiobalises. Aquestes radiobalises retransmeten al satèl·lit el senyal d'auxili i la seva posició als centres de control de missions de rescat. Aquests senyals es fan servir per al rescat tant en terra, mar o aire.

- Transponedors de radar (RESAR)

Són equips que, a bord d'un vaixell o aeronau, i fins i tot en el cas de naufragis, responen en rebre un senyal de radar (d'un altre vaixell o avió) per descobrir la seva posició i així facilitar el rescat.

6.3.2.2. Marc competencial

Les competències en ports són de la Generalitat de Catalunya, a excepció dels ports autònoms de Barcelona i Tarragona, que són de titularitat de l'Estat espanyol, malgrat que en els seus òrgans de govern hi ha una representació del Govern de Catalunya.

Les competències en radiofreqüència són exclusives de l'Estat espanyol, com ja s'ha dit anteriorment en aquest document.

6.3.2.3. Escenaris de col·laboració i riscos

En aquest àmbit, un escenari de col·laboració permetria un traspàs ordenat de competències, assumint els sistemes de salvament marítim amb tots els seus actius terrestres, marítims i aeris.

En el cas de l'espai marítim, és prou coneguda l'operativa de ràdio i radar per part dels operadors del sector, ja siguin navilieres, vaixells o ports i, atesa la poca velocitat dels vaixells, es poden fer servir mètodes alternatius. La possibilitat de generació d'interferències que afectin les comunicacions és baixa, tenint en compte el seu abast, la multiplicitat de canals existents i la utilitat d'aquestes comunicacions en el salvament de persones. Seria poc probable que es produís aquesta situació. Un cas molt diferent seria l'aturada de les TIC que operen en els ports i que podria suposar un seriós problema pel que fa a l'entrada i repartiment de mercaderies a través d'aquestes infraestructures. En aquest cas, caldria estudiar vies alternatives, que no són de l'abast de les TIC, per a aconseguir resoldre el problema.

Quant al sistema de rescat marítim es podria descartar, d'entrada, una aturada o sabotatge atesa la seva importància estratègica en la protecció de la vida humana en cas d'accident o necessitats en el mar.

Les comunicacions de dades en els vaixells, pel fet de ser realitzades via satèl·lit, són en la pràctica molt difícilment interferibles o intervenibles.

6.3.2.4. Alternatives

En cas d'interferències en les radiocomunicacions, es poden fer servir multiplicitat de bandes i canals que permetrien esquivar-les, i a més cal tenir en compte que són fàcilment localitzables i identificables.

Alternativament, tots els vaixells coneixen sobradament la utilització de llums, senyals i sons per poder-se comunicar entre ells i els ports.

6.3.3. El transport ferroviari

6.3.3.1. Descripció i emplaçaments

Igual que en el transport aeri i marítim, el transport ferroviari usa una xarxa de comunicació específica per coordinar el trànsit ferroviari. Actualment, per poder circular, tots els trens depenen de la informació que arriba al centre de control via fibra òptica.

Les xarxes ferroviàries de Catalunya (FGC, Metro, Rodalies de Catalunya i Tram) són infraestructures bàsiques per a la mobilitat de persones i béns. En conseqüència, una alteració en el seu funcionament podria generar problemes greus. Els elements fonamentals a considerar, per a cadascuna d'aquestes xarxes, són:

- Els centres de comandament;
- Els dipòsits de material mòbil;
- Les estacions principals i nusos ferroviaris.

Els centres de comandament són els centres des dels quals es controlen i gestionen totes les operacions i sistemes necessaris per al desenvolupament de l'explotació ferroviària de les línies. Si bé es pot plantejar, en les diferents xarxes, una explotació amb comandaments locals, la capacitat en aquest cas queda dràsticament reduïda.

Aquests centres consisteixen en un conjunt de sales interconnectades que concentren els equips i les persones que en garanteixen l'explotació. El temps de reposició d'aquestes instal·lacions és entorn de tres mesos.

En aquests centres es disposa dels elements següents:

- Equips centrals, xarxa de comunicacions;
- Sistema de control de tràfic centralitzat;
- Sistema de control d'estacions, que inclou tots els elements d'interfonia existents a les estacions amb el propi centre;
- Sistema central d'alarmes d'estacions i cotxeres;
- Sistema de radiocomunicacions tren-terra i telefonia alternativa;

- Sistema d'informació al client;
- Sistema de subministrament d'energia.

Els dipòsits de material mòbil són recintes on s'estaciona una part significativa del material mòbil dels diferents operadors, normalment associats a tallers de manteniment o àrees de servei (neteja, repostatge). Una petita part de les flotes s'estaciona en altres llocs (per exemple en terminals, per facilitar l'inici del servei), però en un nombre clarament insuficient per garantir el servei si per algun motiu el dipòsit queda bloquejat o queda danyat el material mòbil. En qualsevol cas, a banda dels riscos de sabotatge, també seria problemàtic, per poder garantir el servei, que hi hagués interferències que no permetessin un bon funcionament de les comunicacions.

Les estacions estratègiques són nusos d'especial importància a la xarxa d'FGC. Existeixen, també, altres serveis sensibles de Ferrocarrils de la Generalitat de Catalunya amb possibles elements a considerar crítics en àmbits comarcals si les TIC es veiessin afectades i no en garantissin el servei.

6.3.3.2. Escenaris de col·laboració i riscos

En un entorn de col·laboració, quan es produeixi el traspàs de les infraestructures ferroviàries entre l'Estat i la Generalitat, caldria tenir en compte que hi ha centres de control actualment situats fora del territori català, com és el centre de comandament de l'AVE (situat a Saragossa). Aquests centres haurien de tenir el seu equivalent a Catalunya.

Des del punt de vista de les xarxes de comunicació i sistemes d'informació, els riscos a tenir en compte serien els relatius als centres de comandament.

Des d'una perspectiva física, caldria tenir en compte el risc de sabotatges tant d'instal·lacions crítiques com d'obstrucció d'accessos.

Per altra banda, existeixen uns riscos identificats i relacionats amb els sistemes d'informació, com poden ser la manipulació de la configuració dels ordinadors centrals de processos, l'accés no autoritzat als sistemes, la difusió de *software* maliciós, la modificació i l'obstrucció de la informació, la denegació de servei o robatori, la filtració i/o la interacció.

6.3.3.3. Alternatives

Per minimitzar els riscos i maximitzar les condicions de seguretat, en l'àmbit de la ciberseguretat es disposa de les mesures següents:

- Segmentació de la xarxa lògica;
- Sistema de protecció de codis maliciosos;
- Execució de còpia de suport;
- Control i restricció d'accés als sistemes i a la informació segons perfil de l'usuari;
- Alta disponibilitat d'equips crítics;
- Control i restricció d'accessos externs.

Aquests serien els primers elements a protegir.

6.3.4. El transport per carretera / logística

6.3.4.1. Descripció

El transport de mercaderies per carretera ha tingut tradicionalment i continua tenint a Catalunya una notable importància en termes comparats. En aquest cas, el transport en ell mateix no té una dependència directa de les comunicacions electròniques, però sí que la tenen les empreses de distribució, com Mercabarna o la Zona d'Activitats Logístiques (ZAL).

Cal destacar que totes les telecomunicacions del Servei Català de Trànsit, dels ajuntaments i de les autopistes per a la senyalització viària, semàfors i gestió dels peatges funcionen a través de fibra òptica. La seva interrupció podria complicar el correcte funcionament de les principals vies de comunicació del país.

6.3.4.2. Escenaris de col·laboració i riscos

Existeix, doncs, un risc associat a la logística necessària per fer arribar les mercaderies i els aliments als comerços. Aquesta logística podria veure's afectada per la impossibilitat d'accedir a les comandes, els destins, els continguts, etc. en cas de fallada dels sistemes d'informació per atacs informàtics, principalment.

També caldria considerar el risc d'aturada de les senyalitzacions viàries. Aquesta aturada podria ser motivada per l'atac dels sistemes d'informació que la fan funcionar o per la impossibilitat de comunicar-se amb els dispositius de senyalització (semàfors, peatges, etc.).

6.3.4.3. Alternatives

Cal considerar els principals centres de distribució de mercaderies, com Mercabarna, com a infraestructures assimilables a infraestructures crítiques i, per tant, assegurar que disposin dels plans de seguretat informàtica necessaris per fer front a possibles ciberatacs.

Així mateix, els sistemes d'informació i telecomunicacions del Servei Català de Trànsit haurien d'estar securitzats per evitar la fallada per un atac informàtic.

6.4. Els serveis essencials

En aquest epígraf analitzarem els problemes de ciberseguretat i la necessitat de transferència de titularitat que plantegen els serveis públics i privats que, per la seva incidència en el funcionament normal de la societat, mereixen la consideració de serveis essencials des de la perspectiva de les TIC.

6.4.1. Els serveis públics essencials

La major part dels serveis públics que presten actualment les administracions en exercici de les competències que tenen atribuïdes estan suportats en informacions i registres de dades que determinen l'abast, l'amplitud, el qui, el com i el quan s'han de prestar.

La irrupció de les noves tecnologies de la informació ha fet que molts d'aquests serveis s'hagin mecanitzat i depenguin en gran mesura de sistemes d'informació on resideixen les dades necessàries per a la seva producció, on es controlen els nivells de servei, on s'avaluen les polítiques aplicades i on es fan els controls legals pertinents.

Així mateix, aquesta mecanització i l'estructura actual de competències descentralitzades de les administracions públiques, fa que, cada cop més, hi hagi una major interconnexió i dependència dels sistemes d'informació de les diverses administracions.

Aquesta interconnexió i dependència entre sistemes es pot produir de les formes següents:

- Dos sistemes d'informació s'intercanvien informacions en temps real a través de processos col·laboratius. Per exemple, l'alta d'un conveni col·lectiu a l'Administració laboral autonòmica dóna d'alta també el conveni en el sistema d'informació de l'Estat que té la competència del registre de convenis.
- Un sistema d'informació accedeix a informacions d'un altre mitjançant processos d'accés i extracció de dades. Per exemple, la consulta de la situació tributaria global d'un ciutadà s'obté gràcies a l'accés als sistemes d'informació de l'Agència Tributària (AEAT).

Tanmateix, a la pràctica alguns processos i serveis públics s'han transferit sense que les administracions receptores tinguessin els recursos tècnics necessaris per absorbir-los. En aquest sentit, encara que les administracions catalanes són de les més tecnificades, tenen molts processos que s'executen amb sistemes d'informació que governa, administra i proveeix l'Administració General de l'Estat.

Un altre factor de complexitat és que el disseny i la determinació de les solucions tècniques interadministratives no estan coordinades des d'un punt de vista global, sinó que són les unitats organitzatives de cada administració les qui determinen el grau i els mecanismes tècnics en què es basarà la seva col·laboració.

Per últim, cal tenir present que el mapa de col·laboracions entre sistemes d'informació és, en aquests moments, molt complex. El nombre d'interconnexions és molt elevat i els actors, molt diversos: l'Administració General de l'Estat, la Generalitat de Catalunya, les diputacions provincials i els ajuntaments, l'Administració de justícia, les universitats, i molts col·legis professionals.

En l'entorn català, existeix una agència que té la competència de gestionar la interoperabilitat administrativa. Es tracta de l'Administració Oberta de Catalunya (AOC), que pot ser un facilitador quant a la coordinació d'un procés de garantia de serveis interconnectats.

Pel que fa a la informació (és a dir, les dades) que pertanyen a les administracions catalanes, estan emmagatzemades en els centres de processament de dades (CPD). Ens

referirem a aquestes qüestions en el apartat següent.

6.4.1.1. Escenaris de col·laboració i riscos

La prestació dels serveis públics essencials per part d'un eventual Estat català tindria com un dels principals riscos la manca d'interconnexió entre els sistemes d'informació de l'Administració de l'Estat espanyol i els de l'Administració catalana, atès que, com s'acaba de dir, la Generalitat de Catalunya té avui una notable dependència dels sistemes estatals per poder exercir les seves competències. Així, en el cas d'esdevenir un nou Estat, a aquestes competències ja esmentades s'hi afegirien les que actualment exerceix l'Estat espanyol.

En un entorn de col·laboració amb l'Estat caldria establir acords d'interconnexió per evitar aquests riscos. Si la col·laboració no fos possible, la Generalitat hauria d'iniciar amb urgència els processos pertinents per generar els registres i les informacions necessàries i poder prestar els esmentats serveis essencials.

6.4.1.2. Alternatives

Com s'acaba de dir, per a fer front a aquests riscos i poder assegurar la provisió dels serveis públics essencials, s'haurien de dissenyar i executar diferents línies d'actuació prèvies a aquesta transició perquè en el moment que es produïssin es pogués estar en disposició de la informació i dels seus processos de creació i gestió.

Les línies bàsiques d'actuació per a garantir aquesta disposició de sistemes serien:

- Construir el mapa d'informacions bàsiques (inventari) necessari per prestar els serveis essencials i precisar quina és actualment l'administració competent.
- Determinar quins són els sistemes d'informació que contenen aquestes informacions, a qui pertanyen i quina dependència tenen per tal de poder fer un pla de substitució o racionalització.
- Construir sistemes bàsics que suportin els processos de generació i manteniment d'aquelles informacions que avui no es generen dins l'àmbit català.
- Definir un ens que coordini tot el procés i que sigui garant de l'arquitectura d'informació de les administracions catalanes.

6.4.2. Les dades dels serveis públics de les administracions catalanes

6.4.2.1. Descripció

Dins dels sistemes d'informació que cal protegir es troben els centres de processament de dades (CPD). Aquests centres són instal·lacions on s'emmagatzema digitalment el gruix de la informació relativa a la prestació de serveis en el país. Aquestes dades ordenades constitueixen la informació que, degudament processada, permet el desenvolupament de les activitats bàsiques del dia a dia. Per a un Estat, les dades relatives a les persones, el territori i l'activitat econòmica, són fonamentals per al seu desenvolupament quotidià, així com per a la programació, la previsió i l'anàlisi en els processos de presa de decisions.

Catalunya s'està convertint en un nucli de centres de processament de dades del sud d'Europa. Des de l'inici de la crisi econòmica, per motius d'eficiència econòmica i operativa, s'han impulsat processos de concentració de dades en grans centres.

En aquest sentit, les dades vitals de la Generalitat de Catalunya i dels grans consistoris de Catalunya-Barcelona i la seva Àrea Metropolitana, Girona, Tarragona i Lleida- poden ser de gran importància per al manteniment dels serveis bàsics. La informació sobre serveis i processos es podria regenerar amb el coneixement sobre les dades d'una manera més o menys ràpida. Sense dades no existeix informació, i per tant coneixement, per la qual cosa la reconstrucció de processos i serveis seria molt més difícil. Estem parlant, per exemple, de les propietats de les persones, però també dels títols acadèmics, els vehicles, la historia clínica o els assumptes judicials pendents, entre d'altres. Tot això, naturalment, amb ple respecte dels drets fonamentals de les persones afectades i, molt especialment, del dret a la protecció de dades.

6.4.2.2. Marc competencial

Les dades crítiques relatives a la població són propietat dels municipis encarregats de mantenir les dades sobre els padrons d'habitants, base del cens electoral.

Si bé les dades del Servei Català de la Salut suposen la major base informativa transversal de Catalunya, el control dels padrons per part dels municipis, tot i no ser la base per a la

informació fiscal bàsica, sí que suposa una font de construcció d'informació essencial per a la prestació dels serveis i, si més no, d'identificació i localització de les persones.

La informació sensible sobre el territori és propietat de la Generalitat i dels diferents municipis, malgrat que en l'actualitat la informació territorial oferta per agents privats, com Google, és suficientment exacta i útil per a un cas d'absència d'informació oficial.

El creuament d'informació sobre persones i territori dóna lloc, per exemple, a la informació fiscal sobre el territori per l'assignació de llicències, i és bàsica per a la construcció d'un sistema tributari propi.

6.4.2.3. Escenaris de col·laboració i riscos

La pèrdua de la informació relativa a les persones és un risc greu. La pèrdua de control sobre la identitat de les persones deixaria en una situació de vulnerabilitat els sistemes de seguretat, identificació i localització de les persones, al marge de desactivar els sistemes sanitaris, tributaris, acadèmics i de regulació de la prestació de serveis bàsics. Altrament la pèrdua del control dels padrons i censos municipals significaria la impossibilitat de creuar i construir la informació fidedigna de la població amb les dades del Servei Català de la Salut.

Pel que fa a la informació sobre el territori, si bé no tan greu, la pèrdua de les dades geocodificades de la Generalitat o dels ajuntaments més importants, significaria la impossibilitat de localització exacta d'activitats o llocs de caràcter estratègic, com zones industrials, polígons, ports, aeròdroms o ubicacions d'interès logístic.

6.4.3. El servei postal: correus

6.4.3.1. Descripció

Les comunicacions postals han estat considerades per l'ONU una matèria d'especial rellevància en relació amb els objectius que persegueix la pròpia Organització de promoure la cooperació internacional en els àmbits social, econòmic, cultural i educatiu, entre d'altres.

Així ho posa de manifest el fet que la Unió Postal Universal (UPU) -organisme internacional que promou la cooperació i les bones pràctiques en matèria postal- està vinculada a l'ONU

en virtut d'un acord específic, formalitzat d'acord amb les previsions de l'article 57 de la Carta de les Nacions Unides. En aquest marc, l'UPU ha establert, com un dels principis bàsics en matèria postal, l'anomenat "Servei postal universal" en virtut del qual la població gaudeix del dret a un servei postal universal consistent en una oferta de serveis postals bàsics de qualitat, prestats de forma permanent en tots els punts del territori i a preus accessibles; correspon als països membres determinar l'abast d'aquests serveis postals (Actes aprovades pel XXII Congrés de l'UPU, a Beijing, el 15 de setembre de 1999).

En conseqüència, es pot afirmar que existeix consens en la comunitat internacional sobre la necessitat que els Estats donin satisfacció al dret dels ciutadans a un servei postal universal. És per això que una de les actuacions públiques que ha d'impulsar tot Estat de nova creació és la prestació del Servei postal universal.

Per tant, si Catalunya esdevingués un Estat estaria obligada a prestar el Servei postal universal (SPU). En aquesta prestació les TIC hi estan directament relacionades, atès que garanteixen el servei.

A l'Estat espanyol els serveis de correus i telègrafs han estat recentment liberalitzats, per bé que la prestació del Servei postal universal ha estat atorgada per l'Estat a la Sociedad Estatal Correos y Telégrafos, S.A. per un període de 15 anys, per aplicació de la Llei 43/2010, de 30 de desembre, del servei postal universal, dels drets dels usuaris i del mercat postal.

Tot i que la correspondència postal ha retrocedit en gran mesura, empesa per la penetració dels serveis d'Internet i molt notòriament pel correu electrònic, encara no és negligible.

6.4.3.2. Marc competencial

L'Estat espanyol, com a membre de la Unió Postal Internacional (UPU), és el titular de la competència en matèria postal. La Generalitat no té cap competència i no ha actuat mai en aquest camp.

La pertinença a l'UPU o el reconeixement per aquesta organització d'un determinat territori com a territori postal permet, a més a més, que la *International Organisation for Standardization* (ISO) pugui atorgar a un país o territori un codi d'Internet de país (*country code Top-Level-Domain* o ccTLD), que és un codi de dues lletres. A l'Estat espanyol li

correspon el ccTLD ".es"; a Catalunya li correspondria un altre epígraf, que podria ser l'epígraf .cat, usat des de fa temps en webs, correus electrònics i en la resta d'operacions a la xarxa.

6.4.3.3. Escenaris de col·laboració i riscos

Per mantenir el correcte funcionament del servei postal a Catalunya caldria acordar amb l'Estat el traspàs de la gestió del servei. Si no fos així, el principal risc derivaria del fet que la societat estatal prestatària del servei universal de correus podria paralitzar les seves activitats, impedint l'entrada i sortida de correspondència amb l'estranger i la circulació i distribució de correspondència a l'interior del país.

6.4.3.4. Alternatives

Existiria l'alternativa d'acordar amb alguna o algunes empreses privades de serveis postals la substitució dels serveis de la societat estatal mentre el Govern no organitzi el servei postal de Catalunya.

És important remarcar la necessitat de donar solució als diferents sistemes de cobrament pels serveis prestats (franqueig a màquina, franqueig mitjançant segells i acords de franqueig pagat).

Per als segells es podrien emprar les solucions habituals en casos similars. Inicialment es pot sobrecarregar segells espanyols no expedits que estiguin dipositats a Catalunya, per immediatament procedir a la impressió de segells emesos per la nova Administració. Caldria adoptar mesures per permetre el funcionament de les màquines de franqueig, que és la solució emprada per les grans emissores de correu.

Pel que fa a la sortida de correspondència cap a l'estranger i la rebuda des de l'estranger caldria atendre tots els condicionants internacionals que permeten donar el servei als correus externs i per tal que els correus estrangers distribueixin tot el que es generi a l'interior de Catalunya amb destinació a l'estranger. Hi ha alguns organismes internacionals amb els quals s'hauria de negociar i aconseguir-ne el reconeixement i l'associació:

- UPU (Unió Postal Universal). Seu a Berna, amb 192 països associats. És un procés lent, encara que hi ha vies per assolir-ho.

- Acords REIMS, pels quals els estats es paguen entre ells els serveis postals que es presten, en funció, però, de la qualitat de la prestació. Són acords generals, però negociats país a país, per la qual cosa caldria força temps i moltes negociacions. De fet, hauria de ser una de les primeres figures a incorporar, des del primer moment de la nova situació institucional.
- Acords IPS (Internacional Postal Services), per al seguiment en temps real dels enviaments postals. Inclou fins i tot l'establiment d'antenes de seguiment en tot el territori. Encara que és complex, no seria excessivament difícil perquè tots els països estan interessats a poder fer el seguiment o traçabilitat de determinats enviaments.
- En funció de la integració del nou Estat dins de la Unió Europea, serien necessaris els contactes directes i permanents amb les autoritats europees a Brussel·les per tractar aspectes fiscals (el tractament de l'IVA en els serveis postals és molt complex i encara no és igual a tots els països), duaners i legals (totes les modificacions de les directives postals i els efectes i el desenvolupament en cada país, etc.) entre d'altres.

Quant al servei de telègraf, per bé que encara està en funcionament, el seu ús és molt reduït, per la qual cosa cal entendre que podria no ser una prioritat màxima garantir-ne el funcionament en una primera fase.

Pel que fa a l'Administració postal, en un primer moment i en funció del cessament o no de la prestació dels serveis de correus per part de la Societat Estatal Espanyola, caldria disposar d'una entitat o direcció que coordini la posada en marxa dels serveis transitoris. Posteriorment, caldria preveure l'aprovació d'una llei postal pròpia, la creació del servei postal català, mitjançant l'atorgament de la missió de prestar el servei postal universal a una entitat i l'aprovació del finançament d'aquest servei, així com la creació d'una autoritat postal independent.

6.4.4. Els serveis financers

El sector de les TIC ha mantingut una relació estreta amb el sector financer des de l'aparició dels primers sistemes de computació, a meitat del segle XX. Moltes de les innovacions de

les TIC han servit per millorar processos interns, com la gestió transaccional, la contractació en mercats o la interconnexió amb sistemes de pagaments. Des de la irrupció dels grans ordinadors centrals corporatius *mainframe* a finals dels anys 60, fins a les més recents aplicacions en el núvol, les TIC han anat de la mà de la banca en el seu creixement. També és notable l'evolució de la manera com les entitats financeres es relacionen amb els seus clients, on l'oferta de canals s'ha anat ampliant i avui en dia són moltes les entitats que permeten operar a través d'oficines, caixers, telèfon, Internet, etc.

La forta dependència de les comunicacions electròniques per part del sector financer pren importància en el moment en què el ciutadà interacciona amb els serveis per disposar de diners. Les oficines bancàries i els caixers estan constantment connectats a través d'Internet amb les bases de dades dels bancs.

Els dos aspectes que poden afectar la disponibilitat de serveis financers per part dels ciutadans són la custòdia de les dades per part de les entitats bancàries i la continuïtat de les operacions de les sucursals, els caixers automàtics i els datàfons en ús als terminals de punt de venda. Pel que fa a la custòdia de les dades, les principals entitats de matriu catalana compten amb replicació dels seus centres de dades.

Respecte a la continuïtat de les operacions, el factor clau és la disponibilitat de les comunicacions entre els respectius serveis centrals i les seves xarxes d'oficines i caixers. En les entitats considerades, les comunicacions es porten a terme mitjançant xarxes mixtes que combinen línies privades punt a punt i xarxes VPN sobre línies públiques XDSL i XDSI. Per tant, seria aplicable tot el que s'indica en aquest document sobre la integritat dels serveis de telecomunicacions. Per altra banda, la majoria dels caixers tenen una modalitat de funcionament *off-line* que els permet fer operacions –lliuraments de quantitats limitades d'efectiu- en absència de connectivitat, amb posterior compensació de les operacions quan es torna a recuperar.

Aquest tema no hauria de preocupar més enllà d'assegurar que les entitats privades tenen la seva informació protegida davant qualsevol amenaça i es troba replicada de forma segura.

Pel que fa a la Borsa de Barcelona, cal tenir present que tot el funcionament del mercat de valors espanyols està interconnectat. Per tant totes les consideracions respecte de les telecomunicacions i els sistemes, explicades al document també serien d'aplicació pel que fa

a la Borsa. En resum, caldria garantir les telecomunicacions i la protecció contra ciberatacs als sistemes informàtics.

6.4.4.1. Escenaris de col·laboració i riscos

El principal risc de posar en perill el sistema financer seria l'atac informàtic a les bases de dades de les entitats o la Borsa.

6.4.4.2. Alternatives

La principal alternativa seria que les entitats privades disposessin dels seus plans de protecció davant d'atacs cibernètics i que en aquests incloguessin les còpies de seguretat en un altre lloc diferent al principal.

6.4.5. Els serveis d'emergència

L'accés als serveis d'emergència esdevé prioritari per garantir la normalitat en el dia a dia dels ciutadans. Ja s'han descrit parcialment alguns dels possibles problemes en les comunicacions electròniques sobre les quals es sustenten els serveis d'emergència.

Perquè el servei d'emergència funcioni amb total normalitat caldria assegurar tres aspectes:

- Connexió telefònica al 112, 061, 080, 091. És imprescindible que es pugui contactar amb els serveis d'emergència via telefònica. En aquest cas, els riscos i les alternatives corresponen a les ja descrites en l'apartat 6.2.1 sobre telefonia.
- Els diferents cossos haurien de poder disposar de la xarxa RESCAT, mitjançant la qual es comuniquen entre ells, i així poder coordinar les actuacions necessàries. Pel que fa a la comunicació de veu mitjançant la Xarxa RESCAT, els riscos i les alternatives associats s'han descrit en l'apartat 6.2.3 de telecomunicacions.
- Els diferents cossos haurien de poder accedir a les dades necessàries, ja sigui l'historial mèdic, les matrícules de vehicles d'un ciutadà o el seu estat judicial o legal, tot respectant la legislació sobre protecció de dades. Per a tot això cal que les bases de dades siguin accessibles, tal com es descriu en l'apartat 6.4.2 sobre les dades dels serveis públics de les administracions catalanes.

6.4.6. El subministrament energètic

Com passa en molts sectors de la realitat social catalana, el subministrament energètic depèn dels sistemes d'informació per mantenir la seva gestió eficient. Així mateix, cal tenir present que, si bé fan falta els sistemes d'informació per a gestionar el subministrament energètic, l'energia és necessària per al manteniment dels sistemes d'informació.

En termes generals, es pot considerar que el sector de l'energia presenta en aquesta matèria uns trets transversals comuns:

- Es tracta d'un sector en mans d'operadors privats.
- Els operadors es relacionen en règim de lliure mercat (derivat de directives europees).
- Malgrat que es tracta d'un mercat lliure quant a condicions comercials, està fortament regulat especialment quant a condicions tècniques.
- L'operativa en lliure mercat és relativament nova (1997) i està controlada per un regulador únic.
- Majoritàriament, s'han mantingut, latents o operatives, les estructures privades i regulades d'abans de 1997.
- Es tracta d'un sector que té caràcter de "servei essencial". Això significa que, davant incidències excepcionals, la seva protecció permet que els operadors treballin de manera autònoma.

L'estudi monogràfic i detallat d'aquest sector estratègic, on les TIC tenen una forta rellevància, serà objecte d'un proper informe del Consell Assessor per a la Transició Nacional.

6.4.7. Els projectes especials per garantir els serveis essencials

És especialment important que l'Administració catalana pugui disposar d'una base de dades comuna de tota la Generalitat, clau per tenir un cens, per fer una targeta d'identificació

ciutadana o registrar ciutadans i empreses per fer el seguiment de les seves obligacions tributàries (Agència Tributària) entre d'altres actuacions. Aquests projectes haurien d'estar impulsats políticament i per a la seva ràpida i efectiva materialització seria desitjable un entorn de col·laboració amb l'Estat espanyol, a fi que pogués traspassar totes aquelles dades necessàries per al desenvolupament dels diferents projectes i durant el temps que correspongui.

7. El lideratge i la gestió de les TIC

Del que hem dit fins ara es desprèn que en el procés de constitució d'un eventual Estat català caldria que la Generalitat prengués un seguit de mesures específiques per defensar les TIC d'incidents malintencionats que busquin pertorbar l'operativa electrònica normal dels sistemes informàtics o de les seves infraestructures de comunicacions associades. Aquesta actuació suposaria no només garantir tecnològicament la seguretat de les telecomunicacions, sinó també establir mecanismes dirigits a garantir l'abastament energètic imprescindible per al seu funcionament, així com també la seguretat física dels principals nusos de telecomunicacions.

L'abast i la complexitat del problema que caldria afrontar suggereix la necessitat d'un lideratge i gestió d'alt nivell específicament dedicats a la ciberseguretat. En aquest sentit, sembla apropiat comptar amb una estructura de comandament amb responsabilitat sobre la resta d'organismes afectats (com el CTTI, l'AOC i el CESICAT) per tal de coordinar adequadament la ciberseguretat de tots els departaments del Govern i, en general, de totes les TIC que puguin afectar la normalitat de la vida ciutadana.

Abans de l'eventual constitució del nou Estat, la Generalitat tindria ja competència per crear aquesta estructura de comandament que hauria d'actuar, en aquesta primera fase del procés, respectant les competències de l'Estat en matèria de telecomunicacions i, com es obvi, els drets fonamentals dels ciutadans consagrats en la Constitució i les lleis.

8. El paper de la comunicació 2.0 en el procés de Transició Nacional

La comunicació a través dels mitjans digitals pot tenir un paper molt rellevant al llarg del procés de Transició Nacional.

En línies generals, la presència *online* dels organismes de la Generalitat mitjançant servidors web, de correu i altres tipus, que proporcionen als ciutadans informació i serveis en forma d'aplicacions, està raonablement protegida davant possibles atacs de *hacking* (intrusions de tercers per modificar-ne el contingut o el funcionament, o bé per accedir a les dades que contenen) i de DDoS (inutilització per saturació, via una quantitat desmesurada de peticions d'accés).

En tot cas, en paral·lel amb aquesta protecció dels serveis gestionats amb recursos propis, un eventual Estat català hauria d'acceptar el repte de gestionar de manera estratègica tot allò que des de l'acció política i de govern està vinculat amb l'àmbit de les xarxes socials. En un moment en què una part molt important de la ciutadania s'informa i crea continguts a través de les xarxes socials, la gestió estratègica de la presència i el posicionament dels principals actors i institucions del país esdevé un tema central.

En efecte, avui una bona part dels ciutadans rep la seva informació mitjançant les xarxes socials, especialment en moments d'activitat informativa intensa. S'ha comprovat en casos tan diversos com jornades electorals, esdeveniments esportius, accidents o desastres naturals. De fet, el que circula per les xarxes socials acaba en moltes ocasions elevat a la categoria de font informativa per part dels mitjans de comunicació convencionals, incloses la ràdio i la TV, que en multipliquen la difusió. Per això és convenient assegurar una presència adient dels organismes i serveis públics catalans en les principals plataformes 2.0.

D'altra banda, atesa una hipotètica utilització de les xarxes socials per tal de generar desconcert, malfiança i descoordinació entre els actors, les institucions i la ciutadania, seria del tot convenient garantir la presència dels actors, institucions, organismes i serveis públics catalans en les xarxes socials. Les mesures que caldria prendre en consideració serien:

- Assegurar que el Govern, cadascun dels seus departaments, el Parlament, els serveis de protecció civil i mobilitat (Mossos, Emergències, Trànsit) i els individus que puguin ser percebuts com a portaveus autoritzats, són titulars de comptes propis a les principals xarxes socials, els facin servir o no (evitant-ne suplantacions en el darrer cas).
- Elaborar un manual d'actuació per a eventuals suplantacions i segrestaments de la identitat digital, establint un contacte previ amb els gestors de les principals xarxes socials.
- Gestionar la certificació de la titularitat dels perfils i identitats digitals dels actors esmentats, amb l'objectiu de prevenir potencials dubtes de la població i els mitjans sobre l'autenticitat dels missatges que s'emetin.
- Preparar un protocol d'elaboració dels missatges (contingut, freqüència, estil...) que, dins del pla general de comunicació, s'haurien d'emetre a través de les xarxes socials, així com preveure un sistema d'atenció de consultes dels ciutadans i, si escau, la gestió dels rumors infundats i informacions falses.

9. Resum i conclusions

Avui en dia, les societats modernes, com la catalana, viuen en total dependència de la tecnologia. Accions tan quotidianes com veure la televisió, disposar d'efectiu a través del caixer automàtic, consultar les xarxes socials o fer una trucada telefònica, se suporten, en major o menor grau, en sistemes d'informació i xarxes de telecomunicacions, el que s'anomena, genèricament, tecnologies de la informació i la comunicació: les TIC.

Atès que són clau per a la normalitat de la societat, les TIC haurien de poder funcionar sense problemes rellevants i justament per poder garantir aquest funcionament en el moment culminant de la constitució del nou Estat català, si aquesta constitució fos el resultat del pronunciament del poble de Catalunya, és important establir els escenaris de col·laboració adients amb l'Estat espanyol. Un correcte traspàs de competències i de sistemes d'informació fins ara compartits, no només donaria seguretat a la ciutadania sinó que també garantiria la tranquil·litat de tots aquells agents involucrats en les TIC, donant

estabilitat tant al mercat de les telecomunicacions espanyol com al nou mercat català resultant.

Amb aquest objectiu, doncs, cal ser conscients de la importància que prendrien les TIC especialment en la fase final del procés de Transició Nacional des de tres perspectives diferents:

- Les TIC, com a elements que formen part del ciberespai, caldria que fossin protegides davant les amenaces pròpies de la xarxa. Els ciberatacs són una realitat que pot desestabilitzar infraestructures, sectors econòmics i fins i tot governs.
- Les TIC són un actiu que caldria regular de forma ràpida en el moment de la Transició Nacional, respectant sempre, com és natural, els drets dels ciutadans, especialment els relacionats amb la protecció de dades personals.
- Les TIC, en tant que element essencial d'algunes infraestructures, que anomenem crítiques per la seva importància, caldria que fossin protegides d'eventuals amenaces físiques.

9.1. Ciberseguretat

Atesa la importància del ciberespai en la societat actual, el concepte de ciberseguretat cada cop és més present en els àmbits personals, professionals i, sobretot, governamentals.

Existeixen molts casos en què l'atac informàtic ha fet perillar sectors econòmics, infraestructures crítiques o, fins i tot, sistemes d'informació governamentals.

Catalunya és conscient d'aquesta amenaça i des de l'any 2009 disposa d'un Pla Nacional d'Impuls de la Seguretat de les TIC a Catalunya que desplega el Centre de Seguretat de la Informació de Catalunya (CESICAT).

Tot i així, no tots els objectius de protecció estan coberts de forma òptima per aquest organisme. Si bé el perímetre i l'interior de les TIC de la Generalitat estan en constant control i seguiment pel CESICAT i existeix certa col·laboració entre aquest organisme i les forces de l'ordre (Mossos d'Esquadra), falta desplegar més capacitats en el camp de la defensa

cibernètica i de la intel·ligència, entesa com a capacitat d'investigar i prevenir futurs atacs.

Per tal de reforçar aquest aspecte de la ciberseguretat en l'àmbit governamental, caldria prendre en consideració l'adopció de les mesures següents:

- El manteniment de la col·laboració amb els diferents organismes de l'Estat espanyol, com el CCN-CERT i INTECO, per garantir la seguretat de l'espai cibernètic comú; la garantia que els organismes encarregats del desplegament del Pla Nacional de la Seguretat de la Informació puguin defensar el país dels ciberatacs; l'obertura de converses i contactes amb altres equips de resposta d'emergències informàtiques (*Computer Emergency Response Team* – CERT) a nivell català i internacional, per tal de tenir el màxim d'aliats en aquest camp.
- La protecció de les dades públiques dels ciutadans de Catalunya, així com dels centres de processament de dades (CPD) dels quals depèn el Govern, mitjançant l'elaboració d'un Pla de Recuperació de Desastres, amb alternatives, si escau, fora de Catalunya.
- La preparació de les bases de dades per tenir un sistema electoral operatiu, uns documents d'identificació i una Agència Tributària amb les millors garanties d'idoneïtat i correcció en el tractament de les dades dels ciutadans i de les empreses.
- La creació d'una sola estructura de comandament de les TIC a Catalunya que inclogui els principals organismes amb competències en la matèria, com ara la Direcció General de Telecomunicacions i Societat de la Informació (DGTSI), el Centre de Seguretat de la Informació de Catalunya (CESICAT), el Centre de Telecomunicacions i Tecnologies de la Informació (CTTI), l'Administració Oberta de Catalunya (AOC) i l'Agència de Protecció de Dades de Catalunya (APDCAT), entre d'altres. Aquest comandament s'hauria de coordinar amb el Consorci municipalista Localret, diputacions, consells comarcals i ajuntaments pel que fa a l'Administració local, fent un esment especial a la coordinació amb l'Ajuntament de Barcelona per la seva potència respecte a les TIC i la seva ubicació clau en el territori. Aquesta estructura hauria d'estar dotada de mitjans personals i pressupostaris suficients. Abans de l'eventual constitució del nou Estat, la Generalitat tindria ja competència per crear aquesta estructura de comandament,

que hauria d'actuar, en aquesta primera fase del procés, respectant les competències de l'Estat en matèria de telecomunicacions i, com és obvi, els drets fonamentals dels ciutadans consagrats en la Constitució i les lleis.

9.2. El marc normatiu

A la Unió Europea les comunicacions electròniques (telecomunicacions i comunicació audiovisual) funcionen en un mercat liberalitzat, però cada Estat ha regulat aquesta matèria amb la seva pròpia normativa. A l'Estat espanyol, les comunicacions electròniques estan regulades, per un cantó per la Llei 32/2003, de 3 de novembre, general de telecomunicacions (LGTEL) i per l'altre per la Llei 7/2010, de 31 de març, general de la comunicació audiovisual (LGCA).

Pel que fa a l'àmbit de les telecomunicacions, l'article 4 de la LGTEL, obre la porta que el Govern espanyol pugui imposar mesures d'actuació als operadors autoritzats al·legant necessitats de defensa nacional i seguretat pública. Sens perjudici d'això, és complex determinar les mesures que es podrien imposar ja que no n'hi ha precedents. Actualment l'Estat està tramitant una nova llei de telecomunicacions que podria alterar aquest escenari.

En l'àmbit de la comunicació audiovisual, la LGCA reconeix els serveis radiofònics, televisius i connexos i interactius, com a serveis d'interès general que es presten en l'exercici del dret a la lliure expressió d'idees i del dret a comunicar i rebre informació, entre d'altres. Per tant, la prestació d'aquests serveis resta lligada a l'exercici de drets reconeguts en la Constitució.

Només amb la declaració de l'estat d'excepció per part del Govern espanyol, es podrien veure limitats els drets en què es basen les comunicacions audiovisuals i la llibertat de mercat de les telecomunicacions.

En l'àmbit europeu, les directrius sobre la regulació de les telecomunicacions i les comunicacions audiovisuals és més clara que la continguda en l'ordenament espanyol. Ambdós sectors estan patint una convergència tecnològica, que ha de quedar recollida també en una convergència regulatòria.

També des de Brussel·les, es posa molt d'èmfasi en la protecció de les infraestructures

crítiques. La Directiva 2008/114/CE del Consell de 8 de desembre de 2008, sobre la identificació i designació d'infraestructures crítiques europees i l'avaluació de la necessitat de la seva protecció, impulsa la generació de normatives en els estats membres per incloure tots els aspectes de protecció, tant física com cibernètica, de les infraestructures considerades crítiques.

En aquest àmbit caldria prendre en consideració l'adopció de les mesures següents:

- Coordinar amb l'Estat espanyol el traspàs ordenat de competències en matèria de les TIC, vetllant perquè en cap moment no quedi cap competència ni cap contracte en una situació d'inseguretat jurídica.
- Crear un equip legal/tècnic que inicií el procés d'elaboració d'un avantprojecte de llei d'infraestructures crítiques que inclogui, entre d'altres, la seva definició des de la perspectiva de les TIC; l'obligació de les empreses gestores d'elaborar els plans de prevenció i recuperació de desastres; la protecció física i cibernètica d'aquestes instal·lacions; la col·laboració amb el cos de Mossos d'Esquadra i/o empreses de seguretat per garantir la seva integritat física i l'alineament amb el Pla Nacional de Seguretat pel que fa als ciberatacs. Igualment caldria pensar en la conveniència d'instaurar la figura del delegat del Govern en aquestes empreses, en cas d'emergència.
- Crear un equip legal/tècnic que iniciés el procés d'elaboració d'un avantprojecte de decret per regularitzar la relació amb els radioaficionats catalans com a alternativa de comunicació en cas de desastre, en coherència amb la normativa europea que preveu aquesta figura.
- Iniciar la preparació i redacció d'un avantprojecte de llei de comunicacions electròniques (telecomunicacions i audiovisual) per tal d'assegurar la continuïtat legislativa en aquesta matèria.
- Començar a preparar els plans de numeració i freqüències que pertocarien al nou Estat.
- En coherència amb les disposicions europees, valorar la possibilitat d'elaborar una llei per a l'òrgan regulador de les telecomunicacions (actual Comissió del Mercat de les Telecomunicacions - CMT) que en el nou Estat, i a imatge dels països

europeus, hauria de ser la suma de la CMT i del Consell de l'Audiovisual de Catalunya, Telecomunicacions i Audiovisual, conjuntament.

- Iniciar contactes internacionals amb l'organisme regulador de les TIC, la *International Telecomunication Union* (ITU). Així mateix, també seria recomanable establir contactes amb entitats com la *Internet Corporation for Assigned Names and Numbers* (ICANN) i d'altres del sector que ajudessin a preparar els plans tècnics i la legislació, com és habitual a tot el món.

9.3. Audiovisual

La televisió i la ràdio són serveis essencials per a la informació de la ciutadania, però sobretot per a la generació d'un clima de normalitat. Per això, és molt important que el seu servei no es vegi interromput.

A Catalunya, el senyal de ràdio i televisió arriba al 85% de la població gràcies a la Torre de Collserola i a 8 centres reemissors principals. Per arribar al 99,6% de la població, ha estat necessària la instal·lació de 500 torres addicionals.

En aquest àmbit caldria prendre en consideració l'adopció de les mesures següents:

- Coordinar amb l'Estat espanyol el traspàs de l'espectre radioelèctric per al territori català, així com els contractes i drets d'emissió dels diferents grups de comunicació.
- Garantir la seguretat de les infraestructures de telecomunicacions audiovisuals, com la Torre de Collserola, els 8 centres reemissors principals i les 500 torres reemissores disperses pel territori. Si hi hagués un marc de col·laboració, aquesta seguretat es podria garantir amb el suport de l'Estat.
- Iniciar la redacció d'un Pla de Recuperació de Desastres, preveient diverses alternatives i ponderant el seu cost elevat i les limitacions pressupostàries actuals.

9.4. Telecomunicacions

La gran majoria de ciutadans disposa d'un telèfon mòbil, que permet la comunicació de veu i, en molts casos, també la connexió a Internet. Aquesta tecnologia es basa en xarxes i antenes operades per empreses privades a causa de la liberalització del mercat de les telecomunicacions.

A part d'això, la Generalitat de Catalunya disposa d'una xarxa de fibra òptica (XFOCAT), actualment en desplegament, que connectarà la major part de les seves seus i posarà l'excedent d'aquesta xarxa a disposició de les operadores per arribar a qualsevol municipi de Catalunya. Així mateix, pel que fa a Internet, les operadores poden intercanviar les dades amb la "Xarxa de xarxes" a través de punts d'intercanvi de tràfic d'Internet. Catalunya disposa del CATNIX com a punt d'intercanvi de dades d'Internet, on totes les operadores tenen connexió.

També existeix una xarxa de comunicació de veu digital i encriptable, anomenada RESCAT, que serveix per a la comunicació dels serveis d'emergència. Aquesta xarxa utilitza les mateixes infraestructures que la xarxa audiovisual (Torre de Collserola, centres reemissors principals i 500 torres més) per a funcionar.

En aquest àmbit caldria prendre en consideració l'adopció de les mesures següents:

- Acordar amb l'Estat espanyol el manteniment del prefix internacional +34 fins a l'obtenció del propi prefix internacional.
- Protegir la xarxa RESCAT, tot cercant alternatives en cas de desastre.
- Protegir les comunicacions del govern, adoptant les mesures de protecció adients respecte de l'encriptació de veu i dades als nivells que correspongui.
- Desplegar amb la màxima celeritat possible la Xarxa de Fibra Òptica de Catalunya (XFOCAT), sobretot quant als punts estratègics, *backup*.
- Coordinar i elaborar un Pla de protecció de les instal·lacions de cablejat, centrals de veu i dades i torres de telefonia mòbil i Wi-Fi, per tal de protegir-les davant de desastres dins el marc de la Llei d'infraestructures crítiques. Aquest Pla hauria

d'incloure la protecció contra interferències i la certificació de la seguretat en les comunicacions a Catalunya.

9.5. Transports

El transport, ja sigui rodat, ferroviari, marítim o aeri, té una importància cabdal en la normalitat ciutadana i també en la d'aquells que ens visiten. Els mitjans de transport tenen, en major o menor grau, una dependència important de les TIC.

Per una banda, el transport aeri i el marítim depenen de les comunicacions electròniques per a la seva relació amb les infraestructures portuàries i aeroportuàries. Actualment, totes les comunicacions en aquests dos àmbits del sector dels transports estan totalment controlades per l'Estat espanyol. La gran dependència de normatives internacionals, les implicacions en la seguretat dels usuaris i les implicacions econòmiques que representaria un mal funcionament d'aquests transports, són circumstàncies que fan pensar que el funcionament durant la transició seria de plena normalitat.

D'altra banda, el transport ferroviari depèn de centres de control per al seu funcionament correcte, ja que la gestió manual suposaria un funcionament parcial. La seva aturada tindria efectes sobre una gran part de la població, que l'utilitza diàriament, i sobre l'economia.

Finalment, quan s'analitza el transport rodat, cal posar atenció en la senyalització viària que podria deixar de funcionar si hi hagués algun problema amb les TIC que suporten el sistema. També caldria tenir en compte que, cada cop més, el sector logístic i de distribució de mercaderies funciona amb sistemes de comandes i repartiment gestionades amb sistemes d'informació i, per tant, la fallada de les TIC posaria en perill les activitats econòmiques relacionades, per exemple, amb l'arribada d'aliments als punts de venda.

En aquest àmbit caldria prendre en consideració l'adopció de les mesures següents:

- Coordinar amb l'Estat espanyol un traspàs dels actius associats a la navegació aèria, marítima i de transport ferroviari (freqüències, centres de control, salvament marítim, etc.).

- Reforçar la vigilància dels sistemes d'informació i comunicació i les instal·lacions de telecomunicacions, dels centres de control ferroviaris i del Servei Català de Trànsit, per tal de protegir-los d'eventuals ciberatacs i sabotatges.
- Assessorar les empreses públiques i privades de logística i de subministraments per tal de garantir el seu funcionament tecnològic davant de possibles sabotatges.

9.6. Serveis essencials

Actualment, les administracions posseeixen una gran quantitat d'informació de la ciutadania que permet gestionar els serveis que presten en compliment de les competències que tenen atribuïdes. Aquesta informació i registres se suporten avui en dia en centres de processament de dades (CPD), comunament anomenats servidors. Es tracta de les dades del cens, l'historial mèdic, la situació judicial, les dades tributàries o els títols acadèmics d'una persona, entre d'altres.

Alguns dels sistemes d'informació estan sota la tutela o són propietat de la Generalitat de Catalunya o de les administracions locals (com és el cas del padró) i estan ubicats en els CPD que l'Administració catalana té contractats a empreses privades. Però d'altres estan en mans de l'Estat espanyol i la Generalitat en pot consultar els registres. S'ha detectat que fins a 150 aplicacions informàtiques necessàries per al funcionament correcte de l'Administració de la Generalitat depenen de bases de dades ubicades en sistemes d'informació de l'Estat.

Sense ser responsabilitat de l'Administració, existeixen unes altres dades importants: les dades financeres dels ciutadans. Aquesta informació és bàsica, per exemple, per tal que es pugui disposar d'efectiu en un caixer, sempre i que aquest disposi d'una connexió amb la central de l'entitat. Per tant, el sistema financer se sustenta en sistemes d'informació propis on s'emmagatzema la informació i en xarxes de telecomunicacions que connecten les diferents entitats i caixers amb la central. La protecció de les TIC del sistema financer hauria de ser prioritària de cara a garantir el desenvolupament normal de l'activitat econòmica de la ciutadania.

El Servei postal universal, comunament conegut com a Correus, és un dels serveis que tots els estats presten als ciutadans i que en el cas d'esdevenir un Estat caldria prestar.

Actualment, la Generalitat no disposa de cap tipus de control en la gestió de correus en el territori català.

El servei d'emergències esdevé un servei imprescindible i del seu funcionament correcte en depenen serveis com ara la connexió telefònica (en aquest cas, del 112) el funcionament de la xarxa de comunicació de veu RESCAT o l'accés a les dades relatives a històries clíniques, matrícules de vehicles o estat legal dels ciutadans.

L'abastament energètic i d'aigua és també essencial. Si bé la dependència de les TIC d'aquests dos serveis és relativa, ja que es podria funcionar en mode manual, caldria conèixer i tenir a punt el seu funcionament per tal de minimitzar una eventual fallada de les TIC que hi estan relacionades.

Per tant, a l'hora de garantir els serveis públics de l'Administració, el servei de correus, els serveis financers i l'abastament energètic i d'aigua, caldria tenir en consideració l'adopció de les mesures següents:

- Coordinar amb l'Estat la disponibilitat de les bases de dades de la seva titularitat que són necessàries per a la prestació dels serveis públics a Catalunya.
- Protegir les dades públiques dels ciutadans de Catalunya, així com dels CPD dels quals el Govern depèn, elaborant, si escau, un Pla de Recuperació de Desastres prèvia ponderació de la seva viabilitat atesos els costos elevats i les limitacions pressupostàries actuals.
- Coordinar la ciberseguretat per tal de garantir un bon funcionament de tots els serveis públics i privats, incloses entitats financeres, transports, energia, aigua, 012, 112, i qualsevol servei essencial per a la continuïtat de la vida normal dels ciutadans.
- Coordinar les operadores de telecomunicacions amb la finalitat d'assolir els objectius que s'acaben d'esmentar.
- Garantir la continuïtat i el manteniment de totes les aplicacions que actualment estan funcionant, que permeten al Govern realitzar les seves tasques diàries.

- Elaborar una llista completa de les aplicacions informàtiques que en aquests moments són executades des de l'Estat espanyol i que són necessàries per al funcionament del Govern de Catalunya. Alhora, i mentre no es tingui el control definitiu de les aplicacions, adoptar les mesures alternatives per suplir el seu funcionament i pal·liar la manca de les dades que estan dins d'aquestes.
- Elaborar un pla alternatiu al servei de correus estatal espanyol per tal de garantir la continuïtat del servei en cas d'aturada de les seves activitats i preparar el traspàs de les seves competències al nou Estat català.
- Gestionar els dominis d'Internet de la Generalitat i la seva idoneïtat i inviolabilitat a la xarxa.

9.7. Comunicació 2.0

La comunicació a través dels mitjans digitals pot tenir un paper molt rellevant al llarg del procés de Transició Nacional.

En línies generals, la presència *on line* dels organismes de la Generalitat mitjançant servidors web, de correu i altres tipus, que proporcionen als ciutadans informació i serveis en forma d'aplicacions, està raonablement protegida davant possibles atacs de *hacking* (intrusions de tercers per modificar-ne el contingut o el funcionament, o bé per accedir a les dades que contenen) i de DDoS (inutilització per saturació, via una quantitat desmesurada de peticions d'accés).

En tot cas, en paral·lel amb aquesta protecció dels serveis gestionats amb recursos propis, un eventual Estat català hauria d'acceptar el repte de gestionar de manera estratègica tot allò que des de l'acció política i de govern està vinculat amb l'àmbit de les xarxes socials. En un moment en què una part molt important de la ciutadania s'informa i crea continguts a través de les xarxes socials, la gestió estratègica de la presència i el posicionament dels principals actors i institucions del país esdevé un tema central.

En efecte, avui una bona part dels ciutadans rep la seva informació mitjançant les xarxes socials, especialment en moments d'activitat informativa intensa. S'ha comprovat en casos tan diversos com jornades electorals, esdeveniments esportius, accidents o desastres naturals. De fet, el que circula per les xarxes socials acaba en moltes ocasions elevat a la

categoria de font informativa per part dels mitjans de comunicació convencionals, incloses la ràdio i la TV, que en multipliquen la difusió. Per això és convenient assegurar una presència adient dels organismes i serveis públics catalans en les principals plataformes 2.0.

D'altra banda, atesa una hipotètica utilització de les xarxes socials per tal de generar desconcert, malfiança i descoordinació entre els actors, les institucions i la ciutadania seria del tot convenient garantir la presència dels actors, institucions, organismes i serveis públics catalans en les xarxes socials. Les mesures que caldria prendre en consideració serien:

- Assegurar que el Govern, cadascun dels departaments, el Parlament, els serveis de protecció civil i mobilitat (mossos, emergències, trànsit) i els individus que puguin ser percebuts com a portaveus autoritzats, són titulars de comptes propis a les principals xarxes socials, els facin servir o no (evitant-ne suplantacions en el darrer cas).
- Elaborar un manual d'actuació per a eventuals suplantacions i segrestaments de la identitat digital, establint un contacte previ amb els gestors de les principals xarxes socials.
- Gestionar la certificació de la titularitat dels perfils i identitats digitals dels actors esmentats, amb l'objectiu de prevenir potencials dubtes de la població i els mitjans sobre l'autenticitat dels missatges que s'emetin.
- Preparar un protocol d'elaboració dels missatges (contingut, freqüència, estil...) que, dins del pla general de comunicació, s'haurien d'emetre a través de les xarxes socials, així com preveure un sistema d'atenció de consultes dels ciutadans i, si escau, la gestió dels rumors infundats i informacions falses.

Aquest informe sobre *Les tecnologies de la informació i de la comunicació a Catalunya* ha estat elaborat pel Consell Assessor per a la Transició Nacional, que està integrat per:

Carles Viver i Pi-Sunyer
President

Núria Bosch i Roca
Vicepresidenta

Enoch Albertí i Rovira

Germà Bel i Queralt

Carles Boix i Serra

Salvador Cardús i Ros

Àngel Castiñeira i Fernández

Francina Esteve i García

Joan Font i Fabregó

Rafael Grasa i Hernández

Pilar Rahola i Martínez

Josep Maria Reniu i Vilamala

Ferran Requejo i Coll

Joan Vintró i Castells

Víctor Cullell i Comellas
Secretari

Edició revisada: octubre 2014.