ADMINISTRACIÓ ELECTRÒNICA I INTERCONNEXIÓ DE FITXERS ADMINISTRATIUS A L'ESTAT EN XARXA

Pierre Trudel*

Sumari

* Pierre Trudel, professor titular de la Càtedra L.R. Wilson sobre Dret de les Tecnologies de la Informació i el Comerç Electrònic <chairelrwilson.net >, Centre de Recerca de Dret Públic, Facultat de Dret, Universitat de Montreal, <pierre.trudel@umontreal.ca>.

Article rebut el 31.05.2007

La mutació de l'Estat deriva particularment de l'accés a les tecnologies en xarxa. L'inici de l'Administració electrònica és característica de les mutacions induïdes en el dret pels recursos a les tecnologies de la informació per assegurar el funcionament dels serveis governamentals. L'univers postmodern característic dels països afectats per la revolució digital es reflecteix en la morfologia del dret[1]. Com a conseqüència, es deriva una redefinició de les condicions de la intervenció jurídica i les formes de concebre el dret. Una redefinició d'aquestes característiques concerneix en primer lloc les pràctiques relatives a la protecció de les dades de caràcter personal que estan en possessió de l'Administració.

Aquest estudi s'ha dut a terme des de la perspectiva canadenca. Canadà és un Estat federal. Els texts constitucionals divideixen la totalitat dels poders d'aprovar lleis entre el Parlament federal i les legislatures de les províncies[2]. Segons la tradició del govern parlamentari britànic introduïda al Canadà al segle XVIII, els ministeris són responsables dels documents i de la informació que estan en la seva possessió. L'accés als serveis en línia presenta un repte addicional: assegurar els serveis integrats respecte a les matèries que poden dependre de la competència d'entitats que pertanyen a nivells múltiples de govern.

Des del punt de vista dels ciutadans i els administrats, les interaccions amb les instàncies estatals que depenen del Parlament federal i de les legislatures provincials suposen múltiples intercanvis d'informació. Per exemple, per obtenir un passaport, el ciutadà canadenc ha de presentar la informació necessària per acreditar la seva ciutadania. Per fer-ho, haurà de presentar un document de l'estat civil que solen emetre les autoritats que depenen de les províncies. Aquest és només un exemple de les diverses situacions en les quals estan implicades una pluralitat d'instàncies governamentals dependents de l'estat federal o d'una província. En els seus camps respectius de competències, les províncies i el Parlament federal han aprovat lleis relatives a la protecció de les dades de caràcter personal. La protecció de les dades personals està regida per texts que distingeixen entre el sector privat i el sector públic. Els mecanismes de protecció mínims estan dictats en els texts relatius al sector privat. De les lleis es deriven proteccions reforçades que s'apliquen a les entitats que depenen de l'Estat o del sector públic.

Per poder explicar els marcs jurídics relatius a la interconnexió de fitxers administratius en l'Estat en xarxa, en primer lloc és important recordar els imperatius de l'administració electrònica. Després es prendran en compte les exigències relatives a la protecció de dades de caràcter personal i es presentarà el règim jurídic dels intercanvis de dades previst per les lleis sobre la protecció de dades de caràcter personal. Per últim es presentaran els models emergents de mecanismes jurídics destinats a assegurar la compartició etiquetada de les dades personals entre una pluralitat d'entitats de l'Estat.

---

1 Chevalier, Jacques, *L'État post-moderne*, 2a edició, París LGDJ, 2004; Morand, Charles-Albert, *Le droit néo-moderne des politiques publiques*, París LGDJ, 2000.

2 Brun, Henri i Guy Tremblay, *Droit constitutionnel*, 3a edició, Cowansville, Éditions Yvon Blais, 1997, p. 457 i s.

1. Els imperatius de l'Administració electrònica

Els punts clau que marquen el desenvolupament del dret relatiu a l'administració electrònica es basen en l'ajust dels principis jurídics amb l'objectiu d'emmarcar les interaccions en línia. El marc jurídic de l'administració electrònica està marcat per les visions de gestió de l'Estat[3]. Les polítiques d'implantació de l'administració electrònica o de "l'administració en directe" es conceben segons una lògica de reconfiguració de l'oferta de serveis de l'Estat en funció d'una aproximació basada en el ciutadà considerat com un "client".

Kenneth Kernaghan i Justin Gunraj sostenen que l'increment en l'adopció de les tecnologies de la informació per part de les administracions governamentals predisposa els organismes públics a canviar les seves estructures i les seves formes de gestió[4]. Un primer factor de canvi introduït per les tecnologies de la informació és la pressió engendrada per les fortes inversions i el consegüent moviment cap a una cooperació més intensiva entre els organismes governamentals. Un segon factor insisteix en la necessitat creixent d'avaluació i de capacitats majors de compartir la informació. Tot això porta a la creació d'entitats no ministerials. D'aquesta manera, a Canadà s'han creat unes "agències" que es presenten com a estructures amb característiques més adaptades al compliment de funcions horitzontals. Un tercer factor de canvi seria el desplaçament d'una part del nivell intermediari de gestió en benefici d'una certa horitzontalitat de la jerarquia administrativa, l'autoritat i els controls. Juntament amb l'accentuació de les possibilitats de diàleg directe amb els administrats, aquest factor comporta el replantejament dels enfocaments sobre els quals es fonamenten els mecanismes de protecció de dades de caràcter personal en possessió de l'Administració governamental.

Les interconnexions són un component destacable de l'Estat en xarxa. Els intercanvis d'informació hi són constants i no es pot suposar que aquests intercanvis es donen en un espai territorial o organitzatiu determinat. Per exemple, el funcionament de la major part dels serveis en línia es basa en l'hipertext. Això permet i generalitza les possibilitats d'intercreativitat, d'interrelacions i d'intercanvi d'informacions. A partir d'ara les informacions estan tant aquí com en altre lloc al mateix temps, fins i tot en una o en diverses pantalles d'ordinador, de televisió, de ràdios digitals o de telèfons mòbils. Un entorn d'aquestes característiques suposa una compartició major d'informacions, però etiquetades.

---

3 Chevallier, Jacques, «La juridicisation des préceptes managériaux», vol. 11, *Politique et management public*, 1993, p. 111-134.

4 Kernaghan, Kenneth i Justin Gunraj, «Integrating information technology into public administration: Conceptual and practical considerations» vol. 47, *Canadian Public Administration*, 2004, p. 525-546.

La generalització de les plataformes de compartició d'informació posa a l'abast dels usuaris i de les administracions un conjunt de possibilitats d'intercanvi d'informacions. Els internautes, els ciutadans gestors i els agents de l'Estat poden comunicar, compartir i intercanviar informació. Tenint en compte aquest context, el marc jurídic relatiu a la informació que està necessàriament en possessió de l'Administració hauria de regir les condicions d'accés de cada agent de l'Estat més que prohibir-ne la circulació. En un Estat en xarxa, la qüestió no és tant saber si una informació pot estar o no en possessió de l'Administració, sinó si l'Administració té el dret d'accedir-hi i d'usar-la per prendre una decisió en una situació concreta.

Les interaccions en el context de les xarxes informàtiques requereixen modalitats diferents de gestió de la informació. Les administracions funcionen cada vegada més seguint una lògica de xarxa i les informacions són principalment circulants, disponibles en el moment en què han d'estar-ho per complir una prestació de servei. Les condicions de circulació creixent de les informacions també necessiten que es prenguin precaucions, ja que les possibilitats d'acumulació i d'acoblament de la informació són cada vegada més considerables. Aquesta situació ens convida a una actitud realista i a tenir en compte tant els avantatges de la circulació de la informació com els inconvenients.

2. Els imperatius de la protecció de la vida privada i les dades de caràcter personal

La protecció de la vida privada i de les dades de caràcter personal s'identifica normalment com una de les qüestions més importants del desenvolupament de l'administració electrònica. A l'àmbit federal, la *Loi sur la protection de renseignements personnels* (Llei de protecció de dades de caràcter personal), que va entrar en vigor l'1 de juliol de 1983, gestiona la protecció de les dades de caràcter personal en el sector públic federal[5]. Aquesta llei persegueix el doble objectiu de protegir les dades personals[6], mitjançant la limitació de la recopilació, utilització i comunicació de dades, i assegurar el dret d'accés i correcció dels individus a les dades personals que els concerneixen[7] que estan en possessió de les organitzacions federals. Per tant,

5 *Loi sur la protection des renseignements personnels,* L.R., 1985, c. P-21.

6 L'expressió "dades personals", definida a l'article 3 de la llei, s'interpreta de la següent manera en *Dagg c. Canada (Ministre des Finances)*, [1995] 3 C.F. 199 (C.A.) i en *Canada (Commissaire à l'information) c. Canada (Commissaire de la Gendarmerie royale du Canada)*, [2003] 1 R.C.S. 66: per dades personals s'entén qualsevol informació sobre un individu identificable relativa a les seves característiques personals, educació, historial mèdic, antecedents penals, qualsevol número o símbol o altra indicació identificativa, adreça, empremtes digitals, grup sanguini, opinions o idees personals, qualsevol correspondència de caràcter implícitament o explícitament privat o confidencial, idees o opinions d'altres sobre ell, el seu cognom quan es menciona amb altres dades sobre ell o quan la simple divulgació del seu cognom revelés dades sobre la seva persona. En la llei quebequesa la noció de dades personals té un espectre molt ample. L'article 54 indica que "en un document són personals les dades que concerneixen una persona física i permeten identificar-la" i són dades considerades per llei "confidencials tret que la seva divulgació estigui autoritzada per la persona interessada".

7 Aquests dos objectius estan enunciats en les següents decisions: *Dagg c. Canada (Ministre des Finances)*, [1997] 2 R.C.S. 403; *Lavigne c. Canada (Commissariat aux langues officielles)*, [2002] 2 R.C.S. 773

s'aplica a les institucions federals, és a dir, a qualsevol ministeri o departament de l'Estat que depèn del govern de Canadà o qualsevol organisme inclòs en l'annex de la llei, el que representa uns 150 ministeris i organismes federals.

Les províncies i els territoris també han adoptat lleis sobre la protecció de les dades personals[8]. De la mateixa manera que la legislació federal, aquestes lleis regeixen la recopilació, la utilització i la comunicació de les dades de caràcter personal en possessió del organismes dependents tant dels governs provincials com locals. Confereixen a les persones el dret a sol·licitar l'accés a les seves dades personals i a rectificar-les quan escaigui. La vigilància de l'aplicació d'aquestes lleis està generalment assegurada per un comissari, un *ombudsman* o una comissió independent que tingui el poder de rebre queixes i dur a terme investigacions[9].

D'aquests texts legislatius, tant a l'àmbit federal com provincial, es desprenen diversos principis relatius al consentiment, la limitació de la recopilació, la utilització i la comunicació de dades de caràcter personal, els drets d'accés i de correcció dels interessats per les dades i, per últim, a l'exercici d'un recurs independent.

Les excepcions al principi de confidencialitat de les dades de caràcter personal estan limitades als casos en els quals les dades són necessàries per lluitar contra el crim, en les situacions d'urgència en les quals la seguretat o la vida de l'interessat estigui en perill i amb propòsits d'estudi o de recerca. Les altres excepcions importants a la confidencialitat de les dades de caràcter personal són les relacionades amb els acords de transferència d'aquestes dades entre organismes. Són aquests mecanismes els que semblen tenir la intenció d'evolucionar per reflectir els imperatius de l'Estat en xarxa.

---

8 Els principals texts de cadascuna de les províncies i territoris són: **Quebec**: *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (L.R.Q., c. A-2.1); **Ontàrio**: *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31; *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56; **Colúmbia Britànica:** *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165; **Alberta:** *Freedom of Information and Protection of Privacy Act*, R.S.A 2000, c. F-25; **Saskatchewan:** *Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01; *The Local Authority Freedom of Information and the Protection of Privacy Act*, S.S. 1990-91, c. L-27.1; **Manitoba:** *Freedom of Information and Protection of Privacy Act*, S.M. 1997, c. 50; **Illa del Príncep Eduard**: Freedom of Information and Protection of Privacy Act, S.P.E. I. 2001, c. 37; **Nova Brunsvic**: *Protection of personal Information Act*, S.N.B. 1998, c. P-19.1; **Nova Escòcia**: *Freedom of Information and Protection of Privacy Act*, S.N.S. 1993, c. 5; **Terranova i Labrador**: *Access to information and Protection of Privacy Act*, S.N. 2002, c. A-1.1; **Yukon**: *Access to information and Protection of Privacy Act*, R.S.Y 2002, c.1; **Nunavut**: *Access to Information and Protection of Privacy Act (Nunavut)*, S.N.W.T. 1994, c. 20; **Territoris del Nord-oest**: *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20.

9 Per obtenir una descripció del conjunt de les lleis canadenques sobre la protecció de les dades de caràcter personal, consulteu McIsaac, Barbara; Rick Shields i Kris Klein, *The law of privacy in Canada*, looseleaf edition, vol. 1, Scarborough (Ontàrio), Thomson/Carswell, 2000.

3. La compartició de les dades de caràcter personal entre les administracions

Les legislacions relatives a la protecció de dades de caràcter personal en possessió de les autoritats governamentals consagren el principi segons el qual cada organisme públic és una entitat autònoma i responsable de la protecció de les dades personal que té en possessió[10]. A la llum de l'experiència de l'aplicació de les lleis de protecció de dades de caràcter personal, està comprovat que les disposicions que preveuen la possibilitat que un organisme comparteixi algunes informacions personals tot respectant les condicions enunciades són necessàries per al funcionament adequat dels serveis públics. Aquesta necessitat és especialment evident quan es tracta d'assegurar la prestació en línia de serveis personalitzats al ciutadà.

La circulació de les dades de caràcter personal entre les entitats governamentals està regida bé per les disposicions de la llei que permeten la transmissió amb les condicions que hi precisa, bé pels acords o bé per la regla del consentiment explícit de la persona concernida per les dades.

Es preveuen tres mecanismes per emmarcar la compartició de dades personals entre les entitats governamentals. Evidentment, l'interessat també pot autoritzar aquesta comunicació. No obstant, hi ha habilitacions previstes expressament per les lleis en virtut de les quals les dades de caràcter personal es poden comunicar a altres administracions. Un conjunt de regles emmarquen els acords de compartició de dades de caràcter personal entre les entitats governamentals.

3.1. La comunicació efectuada amb el consentiment de l'interessat

El consentiment és la manifestació de la voluntat d'una persona de subscriure un acte jurídic. Respecte a les dades de caràcter personal, el consentiment comprèn l'ús que es pot fer. El consentiment és necessari per autoritzar l'ús de les dades de caràcter personal durant les diferents etapes del seu cicle de vida. Perquè sigui vàlid, el consentiment ha de ser manifest, lliure i explícit, per a finalitats específiques, per una durada determinada i expressat per l'interessat.

Perquè sigui vàlid, el consentiment l'ha de donar l'interessat. L'interessat ha de ser capaç, és a dir, ha de tenir la facultat de ser titular dels drets i d'exercir-los per ell mateix. No obstant això, tenint en compte les conseqüències de l'edat i de la deterioració de l'estat físic o mental de l'interessat, s'han previst mesures de protecció per garantir els interessos dels menors i d'alguns majors. En aquest cas, el consentiment el donen terceres persones. Evidentment, el consentiment es pot sol·licitar i donar en línia. D'altra banda, un dels avantatges més prometedors associat a les prestacions electròniques dels serveis

10 Doray, Raymond i François Charette, *Accès à l'information, Loi annotée, Jurisprudence Analyse et commentaires*, Cowansville, Éditions Yvon Blais, 2001, actualitzat el 15 de novembre de 2006, p. III/59-2.

públics és la capacitat major de diàleg entre el ciutadà-usuari i l'Administració durant les interaccions en línia.

El consentiment ha de ser lliure i explícit. Això significa que ha de donar-se sense cap coacció i amb coneixement de causa. Per tant, l'entitat que recull les dades de caràcter personal té l'obligació d'informar l'interessat de tots els fets pertinents relatius a les activitats per les quals es sol·licita el seu acord. L'exigència del caràcter manifest significa que el consentiment es pot donar verbalment o per escrit, a condició que sigui evident i clar que la persona ha consentit en l'ús o la divulgació d'informació[11].

El consentiment es dona per a finalitats específiques i per una durada limitada. Una vegada el propòsit s'ha acomplert, ja no es deurien utilitzar les dades personals, excepte per obtenir un nou consentiment de l'interessat o de qualsevol altra persona autoritzada per llei. El mateix criteri s'aplica si el posseïdor de les dades de caràcter personal vol utilitzar-les per a una altra finalitat diferent a la prevista inicialment.

No obstant això, hi ha excepcions a aquesta exigència de consentiment per a la transferència o comunicació de dades de caràcter personal. Una disposició legislativa o l'ordre d'un tribunal poden permetre la divulgació o la transferència de dades de caràcter personal sense necessitat de consentiment.

3.2 Les habilitacions generals per compartir les informacions personals

Els organismes públics estan capacitats per llei per compartir dades de caràcter personal quan aquestes dades són necessàries per lluitar contra el crim[12] o en situacions d'urgència on la seguretat o la vida de l'interessat estigui en perill.

Les disposicions preveuen que un organisme públic pugui comunicar, a qualsevol persona o a un altre organisme públic, una informació nominativa sense l'acord de l'interessat si aquesta divulgació és necessària per a l'aplicació d'una llei. Aquesta disposició està formulada de la següent manera:

> ***67.*** *Un organisme públic pot, sense el consentiment de l'interessat, comunicar informació nominativa a qualsevol persona o organisme si aquesta comunicació és necessària per a*

---

11 La *Loi sur la protection des renseignements personnels et les documents électroniques* [Llei de protecció de dades de caràcter personal i documents electrònics] a l'article 4.3.7 de l'annex preveu que el consentiment, necessari des de la recopilació de les dades personals, pot revestir diferents formes, tenint en compte que segons l'article 4.3.4 de l'annex "la forma del consentiment que l'organisme vol obtenir pot variar segons les circumstàncies i el caràcter de les dades". D'aquesta manera, el consentiment haurà de ser explícit si les dades són considerades confidencials. Normalment, un consentiment implícit serà suficient si les dades són considerades menys confidencials. La llei precisa, però, que totes les dades poden esdevenir confidencials després de la recopilació. Sembla, doncs, que l'apreciació del grau de confidencialitat de les dades es deixi als organismes que les recopilen.

12 Frater, Robert, «Should the left hand get what the right hand got? Government information sharing, criminal investigation, and privacy rights», vol. 20, *Supreme Court Law Rev*., 2003, p. 197-212.

> *l'aplicació d'una llei a Quebec, tant si aquesta comunicació està prevista expressament per la llei com si no.*

Des del dia següent de l'entrada en vigor de la Llei, la Comissió d'accés ha mostrat una tendència per mantenir una interpretació restrictiva de la noció de necessitat per a l'aplicació d'una llei. Encara que sigui necessari demostrar que la comunicació d'aquestes dades és "indispensable, essencial i primordial". Doray i Charrette recorden que segons aquesta estricta interpretació "[…] és essencial que una llei mencioni expressament que un organisme públic ha de comunicar les informacions nominatives a una persona o a un organisme públic o privat perquè l'article 67 es pugui aplicar"[13]. Les esmenes introduïdes l'any 2006 van terminar amb aquesta tendència en precisar que no és necessari que la comunicació estigui prevista expressament per llei.

Entre les excepcions previstes del caràcter confidencial de les dades personals, estan les disposicions que autoritzen la comunicació a un organisme d'un altre govern. El paràgraf 68(1r) de la llei quebequesa indica que un organisme públic pot comunicar informació personal "a un organisme d'un altre govern si aquesta comunicació és necessària per a l'exercici de les atribucions de l'organisme receptor o per posar en funcionament un programa gestionat per aquest organisme".

El paràgraf 68(1.1r) preveu que un organisme públic pugui comunicar informació personal "a un organisme d'un altre govern si aquesta comunicació és inequívocament en benefici de la persona interessada". Igualment, el paràgraf 68(3r) autoritza la comunicació d'informació personal:

> *a una persona o a un organisme si aquesta comunicació és necessària en el context de la prestació d'un servei a la persona interessada per part d'un organisme públic, especialment amb l'objectiu d'identificar aquesta persona*.

Pel que respecta a les comunicacions a l'exterior del Quebec, "l'organisme públic ha d'assegurar-se que tindran una protecció equivalent a la prevista en la present llei"[14]. Si l'organisme públic estima que les informacions privades "no tindran una protecció equivalent a la prevista en la present llei, ha de negar-se a comunicar-les o negar-se a confiar a una persona o organisme a l'exterior de Quebec la tasca de gestionar-les, utilitzar-les o comunicar-les pel seu compte"[15].

---

13 Raymond Doray i François Charette, *Accès à l'information, loi annotée, jurisprudence et commentaires*, Cowansville, Éditions Yvon Blais, 2002, p. III/67-2.

14 Art. 70.1 al 1, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Llei d'accés als documents dels organismes públics i la protecció de dades de caràcter personal), (L.R.Q. A-2.1)

15 Art. 70.1 al 2, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (Llei d'accés als documents dels organismes públics i la protecció de dades de caràcter personal) (L.R.Q. A-2.1)

3.3. Els acords de compartició

Les condicions de compartició de dades estan normalment regides per acords entre els organismes implicats. Només la llei quebequesa especifica els elements que han de figurar en els acords. Perquè els acords puguin intervenir entre el govern de Canadà i el govern d'una de les províncies, el Secrétariat du Conseil du Trésor ha emès unes directrius per als ministeris i organismes federals sobre els elements que han de contenir aquests acords[16]. Els acords d'intercanvi de dades personals han d'incloure:

- una descripció de les dades de caràcter personal que es compartiran;
- els objectius pels quals les dades es comparteixen i s'utilitzen;
- un enunciat de totes les mesures de protecció administratives, tècniques i materials necessàries per a la protecció del caràcter confidencial de les dades, sobretot en el que concerneix al seu ús i comunicació;
- un enunciat que precisi si les dades rebudes per la institució federal estaran subjectes a les disposicions de la Llei de protecció de dades de caràcter personal (per exemple, si els interessats poden tenir accés a les dades i, si no, quines excepcions es recomanen per a la institució que proporciona les dades);
- un enunciat que precisi si les dades comunicades per la institució federal estaran subjectes a les disposicions de la Llei de protecció de dades de caràcter personal (per exemple, si la institució que rep les dades pot donar-hi accés als interessats i, si no, quines excepcions es recomanen);
- un enunciat que indiqui que la compartició de dades terminarà si el beneficiari comunica de manera inoportuna les dades de caràcter personal compartides;
- el nom, el títol i la signatura de l'agent autoritzat de la institució que proporciona les dades de caràcter personal i de la que les rep, així com la data de l'acord.
-

Al Quebec, el règim d'acords de compartició de dades de caràcter personal està definit més concretament en els articles 67 i posteriors de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Llei sobre l'accés als documents dels organismes públics i sobre la protecció de les dades personals). La transmissió d'informacions personals ha d'estar emmarcada per acords amb les finalitats del compliment d'un mandat. Els articles 67.2 i 67.3 preveuen que un organisme públic pot, sense el consentiment de l'interessat, comunicar informació nominativa a qualsevol persona o organisme si aquesta comunicació és necessària per a l'exercici d'un mandat confiat per l'organisme públic a aquesta persona o aquest organisme. En aquest cas, l'organisme públic ha de: en primer lloc, confiar aquest mandat per escrit i, en segon lloc, consignar un conjunt d'indicacions.

16 Canadà, *Secrétariat du Conseil du Trésor, Politiques et Lignes directrices* : *Formulaires - Protection des renseignements personnels - 3-05*. En línia: http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/siglist_f.asp.

L'organisme ha d'indicar, en aquest mandat, les disposicions de la llei que s'apliquen a la informació que ha estat comunicada així com les mesures que s'han de prendre perquè aquesta informació no s'utilitzi en l'exercici del mandat. S'ha de precisar que les dades de caràcter personal seran destruïdes després de l'expiració del mandat. A més, l'organisme públic ha d'obtenir, abans de la comunicació, un compromís de confidencialitat complimentat per totes les persones a qui es poden comunicar les dades, excepte si el responsable de la protecció de les dades de caràcter personal estima que no és necessari. Una persona o un organisme que exerceix un mandat o executa un contracte de servei inclòs en el primer paràgraf ha d'informar sense dilació al responsable de qualsevol infracció o temptativa d'infracció per qualsevol persona de les obligacions relatives a la confidencialitat de les dades comunicades i també ha de permetre que el responsable efectuï qualsevol verificació relativa a aquesta confidencialitat.

El registre dels acords de compartició d'informacions personals comprenen precisions sobre:

1 *la natura o el tipus de dades comunicades;*
2 *la persona o l'organisme que rep aquesta comunicació;*
3 *la finalitat amb la qual es comuniquen aquestes dades i la indicació, si s'escau, que es tracta d'una comunicació inclosa en l'article 70.1;*
4 *la raó que justifica aquesta comunicació;*

En el cas d'un acord sobre la recopilació de dades personals, el registre comprèn:

1 *el nom de l'organisme per al qual es recopilen les dades;*
2 *la identificació del programa o de l'atribució per al qual les dades són necessàries;*
3 *la natura o el tipus de prestació de servei o de missió;*
4 *la natura o el tipus de dades recopilades;*
5 *la finalitat amb la qual es recopilen les dades;*
6 *la categoria de persones, al si de l'organisme que recull les dades i al si de l'organisme que les rep, que tenen accés a les dades.*

En el cas de la utilització de dades de caràcter personal amb una finalitat diferent amb la qual es van recopilar, el registre comprèn:

1 *la menció de l'apartat del segon paràgraf de l'article 65.1 que permet la seva utilització;*
2 *en el cas previst a l'apartat 3 del segon paràgraf de l'article 65.1, la disposició de la llei que fa necessària la utilització de les dades;*
3 *la categoria de persones que tenen accés a les dades amb la finalitat de la utilització indicada.*

El registre és accessible a tota persona que ho sol·liciti, excepte en relació amb les dades de caràcter personal, la confirmació de l'existència de les quals pot ser rebutjada en virtut de les disposicions de la llei que protegeixen les dades en possessió de les forces policíaques. (art. 67.4)

Com hem senyalat, les disposicions autoritzen la comunicació de dades de caràcter personal a un organisme d'un altre govern. Així, el paràgraf 68(1r) indica que un organisme públic pot comunicar informació personal "a un organisme d'un altre govern si aquesta comunicació és necessària per a l'exercici de les atribucions de l'organisme receptor o el funcionament d'un programa gestionat per aquest organisme". Amb el mateix caràcter, el paràgraf 68(1.1r) preveu que un organisme públic pugui comunicar informació personal "a un organisme d'un altre govern si la comunicació és inequívocament en benefici de l'interessat". Recordem també que el paràgraf 68(3r) autoritza la comunicació d'informació de caràcter personal "a una persona o un organisme si aquesta comunicació és necessària en el context de la prestació d'un servei a la persona interessada per part d'un organisme públic, especialment amb l'objectiu d'identificar aquesta persona".

En els tres casos mencionats anteriorment, la comunicació s'efectua en el context d'un acord escrit. Aquest acord s'ha de sotmetre a la Comissió per al seu dictamen[17]. Quan ha d'emetre un dictamen en relació amb un acord de compartició de dades de caràcter personal, la Comissió ha de prendre en consideració la conformitat de l'acord amb les condicions incloses en l'article 68 o en l'article 68.1, és a dir, que l'intercanvi es refereix a una situació on la comunicació és necessària per a l'exercici de les atribucions de l'organisme receptor o el funcionament d'un programa gestionat per aquest organisme. En altres situacions, caldrà assegurar que la comunicació és en benefici de la persona interessada o és necessària per a l'aplicació d'una llei.

La Llei també demana que la Comissió consideri l'impacte de la comunicació de les dades en la vida privada de l'interessat, si s'escau, en relació amb la necessitat de l'organisme o la persona que rep la comunicació de tenir aquestes dades.

La Comissió ha d'emetre un dictamen motivat en un termini màxim de 60 dies a partir de la recepció de la petició de dictamen acompanyada de l'acord. Si la petició es modifica durant el termini, aquest comença a comptar des de l'última petició. Si no és possible la tramitació de la petició de dictamen en aquest termini sense perjudicar el desenvolupament normal de les activitats de la Comissió, el president pot, abans de l'expiració del termini, prolongar-lo per un període màxim de 20 dies. Ha d'informar les parts de l'acord en el termini de 60 dies.

L'acord entra en vigor amb el dictamen favorable de la Comissió o en la data posterior prevista en l'acord. La Comissió ha de fer públic aquest acord i el seu dictamen. Si no hi ha dictamen en el termini previst, les parts de l'acord estan autoritzades a procedir amb la seva execució.

17 Art. 70, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Llei d'accés als documents dels organismes públics i la protecció de dades de caràcter personal) (L.R.Q. A-2.1).

En cas de dictamen desfavorable de la Comissió, el govern pot, a petició, aprovar l'acord i fixar les condicions aplicables. Abans d'aprovar l'acord, el govern publica a la *Gazette officielle du Québec* l'acord i, si s'escau, les condicions que preveu fixar amb un dictamen que podrà aprovar l'acord quan expiri el termini de 30 dies d'aquesta publicació i que tota persona interessada pot, durant aquest termini, transmetre comentaris a la persona designada. L'acord entra en vigor el dia de la seva aprovació o en la data posterior fixada pel govern o prevista en l'acord. Aquest acord, el dictamen de la Comissió i l'aprovació del govern es presenten a l'Assemblea nacional durant els 30 dies posteriors a l'aprovació si l'Assemblea està en sessió o, si no està reunida, en els 30 dies posteriors a la represa del treball. El govern pot revocar en qualsevol moment un acord d'aquestes característiques[18].

Encara que tinguin dret d'accés als registres que recopilen els acords d'intercanvi de dades de caràcter personal, els ciutadans no estan informats sistemàticament de les conseqüències que aquests acords poden tenir sobre la comunicació secundària de dades personals que han de proporcionar. No hi ha un procés públic d'avaluació que permeti apreciar els impactes, els riscs i els desafiaments que aquests intercanvis poden comportar.

Quan les transmissions s'autoritzen, comporten la possibilitat que l'organisme públic receptor esdevingui el posseïdor de la totalitat de les dades concernides. Per exemple al Quebec, on existeixen disposicions més detallades, el procés d'aprovació per la Comissió, quan ocorre, no està precedit d'un debat públic i controvertit. La Comissió rep una petició i emet un dictamen normalment a partir de la informació proporcionada pel ministeri o organisme pertinent. No hi ha audiència pública en la qual l'organisme públic i els interessats puguin debatre els desafiaments i els riscs.

4. El model de xarxa per explicar la protecció dels drets en els serveis transgovernamentals

Des del punt de vista del ciutadà, l'Estat es presenta cada vegada més com una xarxa en la qual les fronteres administratives semblen tenir cada vegada menys pertinència. Aquest fenomen afavoreix un increment de les responsabilitats reguladores dels actors en primera línia i augmenta la necessitat de desenvolupar instruments per assegurar el desenvolupament d'instruments reguladors apropiats a nivell local i dels microcentres virtuals.

La xarxa substitueix cada vegada més les institucions jerarquitzades com a lloc de concepció i d'enunciació de la normativitat. D'aquí la idea d'una regulació rellevada en diversos vectors. Aquesta tendència fa pensar que les institucions habituades a models flexibles de regulació són les més susceptibles d'actuar amb eficàcia a l'univers digital de l'Estat en línia.

---

18 Art. 70, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Llei d'accés als documents dels organismes públics i la protecció de dades de caràcter personal) (L.R.Q. A-2.1).

La xarxa suposa l'emergència d'espais interconnectats que vinculen responsables, investigadors i reguladors així com altres actors que tenen un paper en el governament dels espais al si dels quals discorren les activitats del governament[19]. És el que trobem als espais d'interacció entre l'Administració i els ciutadans. En el seu "model integrat d'administració electrònica", Réjean Roy inclou la dimensió jurídica al nombre d'elements del marc comú del governament de l'administració electrònica[20]. Les normativitats jurídiques contribueixen amb les normativitats administratives, tecnològiques i polítiques a emmarcar les interaccions i els intercanvis d'informació al si de l'aparell governamental.

Aquest tipus de model rendeix compte de la dimensió en xarxa de l'administració electrònica, del fet que l'espai que ens ocupa és un conjunt interconnectat constituït de pols que interactuen amb normativitats. Està constituït per espais en els quals prevalen completament o parcialment normes que s'imposen als usuaris i altres socis. Les normes poden imposar-se bé per la seva capacitat de definir, fins i tot implícitament, les condicions de l'exercici de les activitats, bé perquè un participant està en condicions d'exercir una autoritat. Aquest espai també està constituït per relleus pels quals s'expliciten i es difonen tant les normativitats com les seves conseqüències. Les regles que emanen dels pols de normativitat es relleven i es difonen als diferents espais virtuals. Coexisteixen bé en complementarietat amb altres regles o bé en competència, quan es proposen en lloc de les regles que han sorgit d'altres pols normatius[21].

La normativitat en xarxa característica dels espais fundats en l'ús de les xarxes de comunicació informàtica comporta canvis en les maneres de concebre el repartiment de les responsabilitats[22]. El model clàssic, característic de l'Estat liberal on cada ministeri o entitat administrativa es considera que té el control complet i exclusiu de les seves dades, està gradualment canviant a un model on la compartició d'informació exigeix aplicar noves formes de distribució i repartiment de responsabilitats.

Si a l'univers burocràtic dominat pel paper el dret insisteix en la delimitació dels drets d'obtenir o no una informació o una altra, a l'univers en xarxa el dret tendeix a l'organització d'una regulació de permisos d'accés i d'ús corresponents als responsables i als ciutadans.

Sembla que es perfila una tendència cap a una evolució de les concepcions que velen per la interpretació dels principis fonamentals relatius a la gestió de les dades personals. Així, la limitació en matèria de recopilació suposa posar en funcionament processos de decisió que utilitzaran la mínima

---

19 Castells, Manuel, *La société en réseaux. L'ère de l'information*, Paris, Fayard, 1998; FRANÇOIS OST i Michel de Kerchove, *De la pyramide au réseau : pour une théorie dialectique du droit*, Brussel·les, Publications des facultés universitaires Saint-Louis, 2002.

20 Roy, Réjean, *Vers un modèle intégré de gouvernement électronique*, Quebec, CEFRIO, 2005, p. 6, < http://www.cefrio.qc.ca/Actes/acte_06.cfm >.

21 Trudel, Pierre, «Un 'droit en réseau ' pour le réseau : le contrôle des communications et la responsabilité sur internet» dans Institut Canadien d'Études Juridiques Supérieures, *Droits de la personne : Éthique et mondialisation*, Cowansville, Éditions Yvon Blais, 2004, p. 221-262.

22 Sobre les mutacions del model piramidal envers un dret en xarxa, vegeu: Bailleux, Antoine, «À la recherche des formes du droit : de la pyramide au réseau», vol. 55, RIEJ, 2005, p. 91-115.

informació necessària per assegurar les prestacions o la presa de decisions. És necessari poder justificar el perquè de la recopilació de cada informació personal.

En un context en xarxa, la necessitat de la recopilació s'ha de contemplar en relació al conjunt de famílies de prestacions concernides per les informacions. Quan la informació s'ha recopilat, la necessitat de la seva conservació es pot apreciar en relació a un conjunt de processos de decisió susceptibles de realitzar-se recurrent a una informació personal. El principi de retenció en matèria de recopilada i el principi d'especificació de les finalitats coincideixen. El principi relatiu a l'especificació de les finalitats també està reforçat: en especificar el més taxativament possible les finalitats, estarem en una situació en la qual la recopilació estarà limitada a les informacions efectivament indispensables a les finalitats perseguides pel pla del conjunt de les prestacions i serveis que hauran d'estar assegurades al si d'una xarxa.

La regla que impedeix la circulació i la reutilització de la informació perquè aquesta informació es podria desviar de la seva finalitat s'ha de situar en el context de major diàleg que permet la xarxa. Més que mai, l'Administració està en condicions d'indicar a cada administrat quina informació té, quina informació pretén utilitzar per prendre una decisió. El ciutadà està d'ara endavant en posició d'interactuar i d'exigir que es retiri o s'afegeixi informació.

La generalització de les xarxes porta a reconèixer la necessitat respecte al conjunt de les situacions concernides per un context d'informació. En efecte, sempre s'ha de considerar la necessitat en el pla de la legitimitat de la recopilació i de la possessió d'informació, com exigeixen els principis actuals. Però també s'ha d'assegurar que només la informació pertinent i autoritzada s'utilitza en el marc d'un procés de decisió específic. Es necessita, doncs, una gestió en què es dissocien, d'una banda, la qüestió de la necessitat de la possessió de la informació i, d'altra banda, l'apreciació de la necessitat d'accedir-hi per una decisió o prestació determinada.

El principi de finalitat implica que només es poden recopilar i utilitzar dades de caràcter personal per a finalitats compatibles amb les de la recopilació inicial. El principi de finalitat està lligat al manteniment de la qualitat de la informació. En els principis de l'OCDE, aquesta exigència s'explica així:

> *Les dades de caràcter personal han de ser pertinents en relació a les finalitats per a les quals s'hauran d'utilitzar i, en la mesura en la qual aquestes finalitats ho exigeixin, hauran de ser exactes, completes i actualitzades.*[23]

En el context d'un espai en xarxa, la qüestió de la finalitat es planteja tenint en compte que la informació pot estar allà disponible, ja recopilada: l'exigència de respectar la finalitat ja no s'aplica tant a la possessió sinó a l'accés i a la utilització de les dades. En una xarxa, el principi de control del dret

[23] OCDE, *Lignes directrices régissant la protection de la vie privée et des flux transfrontières de données de caractère personnel*, Paris, OCDE, 2002, <http://www.oecdpublications.gfinb.com/cgibin/OECDBookShop.storefront/EN/product/932002012P1>.

d'accés assegura que es respecta la finalitat. L'accés a una informació només és lícit per a una finalitat autoritzada i si es realitza una activitat que s'inscriu en el marc de la finalitat.

El respecte al principi de finalitat suposa que efectivament l'usuari té coneixement de les famílies de finalitats a les quals servirà la informació al si de les xarxes dels serveis públics. La noció de finalitat ha d'estar, d'ara endavant, centrada en l'usuari, no en les estructures governamentals. Per exemple, l'usuari que entra en relació amb els ministeris encarregats de l'aplicació de les lleis sobre la seguretat de la renda dels impostos ha de saber que la informació que proporcioni circularà i serà utilitzada amb la finalitat d'assegurar l'aplicació de les lleis relatives a la seguretat dels impostos i que és indiferent que una tingui relació amb un ministeri i l'altra amb un organisme públic tercer. És necessari que la informació sobre les finalitats de les informacions en possessió estigui constantment disponible i en coneixement de l'usuari durant cada recopilació. Per tal de respectar el principi de la limitació de la utilització, els espais d'informació hauran de comunicar les famílies delimitades de prestacions, per assegurar que les dades de caràcter personal seran utilitzades només per a fins relacionats i compatibles amb les de la recopilació inicial.

La transparència és una condició essencial de la credibilitat i de la confiança als espais en xarxa. L'usuari ha d'estar en condicions de saber amb qui té relació i com es concep el procés d'informació en el qual està immers. Per això l'avaluació pública dels espais d'informació o de la compartició d'informació per a finalitats de prestacions electròniques adquireix una major importància. Els desafiaments i els riscs associats a les prestacions electròniques que ens plantegem proposar en xarxa s'han de divulgar i debatre públicament i els seus riscs s'han d'avaluar públicament.

La qualitat de les dades s'aprecia en relació amb les prestacions que s'han d'acomplir: s'ha de garantir que les dades utilitzades per efectuar la prestació són exactes, precises, estan autoritzades per les lleis i no presenten cap equívoc. La legitimitat de circulacions semblants de dades de caràcter personal estan reforçades quan un ciutadà vol revisar i, quan escaigui, rectificar en línia o per una altra via les dades que el concerneixen. El dret de rectificació, fins ara tan poc exercit, aconsegueix un sentit ple.

Com que les dades de caràcter personal estan disponibles en xarxa, cada organisme ha d'assegurar que la informació a la qual pot accedir, per dur a terme una prestació relativa a una persona, té la qualitat adequada, tenint en compte les exigències i el context de la prestació. Per tal d'assegurar la qualitat, és necessari comptar amb el potencial de diàleg en directe entre l'Administració i l'usuari que encobreixen les tecnologies en xarxa.

En aquest aspecte, el principi de la participació individual de l'interessat en les decisions relatives al tractament de les dades de caràcter personal adquireix en la xarxa una nova dimensió. En les xarxes és possible presentar la informació que es té i validar-la en temps real amb l'interessat. La garantia de qualitat de les dades estarà també reforçada per la validació de la informació que l'organisme efectua durant una prestació específica.

Tractant-se de la responsabilitat, cada organisme públic susceptible d'accedir a les dades personals al si d'una xarxa es pot considerar com el detentor jurídic. Per això, cada organisme és responsable de la

confidencialitat de les dades i el conjunt dels organismes responen solidàriament. Com que hi ha una pluralitat d'organismes, aquests hauran de determinar com es repartiran la responsabilitat dels participants. De fet, és important precisar les obligacions i delimitar la responsabilitat dels gestors en relació a les exigències de confidencialitat i de seguretat. Efectivament, és necessari que es precisen les normes en vista de les quals s'avaluaran el comportament i la responsabilitat dels ciutadans i del gestor.

La seguretat tant física com lògica és evidentment una exigència essencial per a qualsevol entorn que funciona en xarxa. El marc jurídic ha d'incitar els responsables a prendre les mesures per garantir la seguretat de les dades sobre les persones. Més enllà d'una cultura de la seguretat, és necessari un conjunt de processos capaços de prevenir els atacs i, sobretot, de solucionar-los en el moment que es produeixi un esdeveniment que posi en perill els processos de tractament.

D'aquesta manera, quan les dades estan en entorns d'informació als que tenen accés una pluralitat de ministeris o altres organismes o entitats públics, la protecció de les dades de caràcter personal ja no resulta de les limitacions que intervenen en l'estadi de la recopilació o que prohibeixen la circulació. La veritable protecció prové d'un marc estricte de condicions per les quals és lícit accedir a les dades i de condicions de la seva utilització. El marc jurídic ha de dissociar la possessió de la informació i el dret d'accedir-hi i usar-la.

En efecte, com que les dades estan en un entorn d'informació accessible a una pluralitat d'entitats, la informació està disponible, però això no atorga, en si mateix, el dret a accedir-hi. L'èmfasi es desplaça cap al dret a utilitzar les dades de caràcter personal més que sobre la sola possessió o retenció de les dades. Hi ha una dissociació entre la possessió física d'una informació per part d'una entitat i el dret d'aquesta d'accedir-hi o d'usar-la. A causa de la seva participació en un espai en xarxa, un ministeri o una altra entitat pública tenen un conjunt d'informacions en comú amb altres entitats. No obstant això, només tenen dret d'accedir a aquestes informacions si és necessari per complir una prestació prevista per l'acte constitutiu d'àrea de compartició.

Finalment, en el context de l'Administració electrònica, les proteccions s'han de concebre per garantir que les dades de caràcter personal seran efectivament utilitzades per a finalitats lícites, més que per impedir la seva circulació. Comencen a emergir models per estructurar els modes de protecció en els espais en xarxa. A Canadà, es parla d'àrees de compartició, un concepte que es conjuga seguint modalitats de geometria variable segons el grau de confidencialitat de les dades i es comencen a prendre mesures de models fonamentats en el domini, per part de l'usuari, de les informacions.

4.1. Les àrees de compartició de les dades de caràcter personal

Ja que la circulació de dades de caràcter personal entre els organismes públics cessa de tenir un caràcter excepcional, és millor disposar d'un marc jurídic decididament centrat en les condicions que s'han de respectar durant el desplegament de prestacions de serveis en línia. També són necessàries garanties durant l'establiment d'espais de circulació de dades personals. Des del punt de vista jurídic, els espais-xarxa en els quals circulen dades personals han d'estar emmarcats per regles que precisen les

responsabilitats del conjunt de les entitats concernides. En suma, es tracta d'establir regles que designen a qui respon de les informacions repartides en xarxa. Per fer-ho, és important rebre les premisses sobre les quals reposen la majoria de les lleis sobre la protecció de dades de caràcter personal que reflecteixen sovint el postulat que la protecció de dades està assegurada pel seu confinament.

L'àrea de compartició és una de les nocions desenvolupades per pensar en els nous models de compartició en els entorns en xarxa. L'àrea de compartició es pot definir com un espai d'informació en el qual les dades de caràcter personal necessàries per a la concessió d'un conjunt de serveis portats a terme en benefici dels ciutadans poden estar disponibles per a diferents entitats[24]. Aquests serveis o prestacions tenen un caràcter complementari i per dur-los a terme són necessàries informacions que estan en possessió d'una pluralitat d'entitats unides per un acord. La noció proporciona un concepte adaptat a les realitats de les xarxes i permet concebre els drets i les obligacions del conjunt de socis de l'administració electrònica.

El concepte porta a un conjunt de mecanismes que senyalen la circulació de la informació i en delimiten els usos. Es tracta d'organitzar l'espai al si del qual poden circular les dades. El marc que es deriva defineix els drets i les responsabilitats. Les proteccions es conceben per garantir que les dades seran efectivament utilitzades per a finalitats lícites, més que per impedir la seva circulació.

4.2. Els repertoris d'informacions personals sobre la salut disponibles en línia amb el consentiment del pacient

Segons diferents condicions, les disposicions incloses en les legislacions de diferents països organitzen l'allotjament i la circulació controlada de les dades sobre la salut per a finalitats assistencials. Per exemple, en la legislació francesa i quebequesa, s'ha instituït un règim jurídic per als espais d'informació en els quals les dades de caràcter personal necessàries per a la concessió d'un conjunt de serveis portats a terme en benefici dels ciutadans poden estar disponibles per a diferents entitats. Les informacions només estan disponibles per als serveis o prestacions de salut que tinguin caràcter complementari. Aquesta disponibilitat d'informacions per a una pluralitat d'entitats –com els metges, altres professionals de la salut o els hospitals– comporta unes condicions estrictes.

En el dret francès és la *Loi relative aux droits des malades*[25] (Llei relativa als drets dels malalts) que introdueix l'article L. 1111-8 al *Code de la santé publique* (Codi de la salut pública). Aquesta disposició organitza el règim jurídic del contracte d'allotjament. En termes de l'article L.1111-8 "la prestació d'allotjament és objecte de contracte". Disposa que:

---

24 En aquest sentit vegeu: Trudel, Pierre, «Renforcer la protection de la vie privée dans l'État en réseau; l'aire de partage de données personnelles», vol. 110, *Revue française d'administration publique*, 2004, p. 257-266.

25 Llei núm. 2002-303, de 4 de març de 2002, D.O. 5 març 2002.

> *Els professionals de la salut o els establiments de salut o l'interessat poden presentar dades personals sobre la salut, recopilades o produïdes en activitats de prevenció, de diagnòstic o de cura, davant de persones físiques o morals admeses a aquest efecte.*

Quan la possessió material de les dades es transfereix a l'entitat responsable de l'allotjament, aquesta es converteix en dipositària. Només les entitats responsables d'allotjament admeses estan autoritzades a tancar un contracte d'allotjament. Per a l'entitat responsable de l'allotjament, la falta de consentiment exposa a una sanció penal i a la nul·litat del contracte. Les parts del contracte són els professionals de la salut, els establiments de salut i l'interessat. L'acord d'aquesta última és una condició de validesa del contracte. Isabelle Vacarie afirma que:

> *Per cada pacient hospitalitzat en un establiment de salut públic o privat, el Codi de la salut pública prescriu la constitució i conservació d'una historia clínica. Però el Codi autoritza l'externalització de les històries a una entitat responsable. En aquest respecte, el codi precisa que "aquest allotjament de dades només es pot donar amb el consentiment exprés de l'interessat". El seu acord és doncs una condició de validesa del contracte. El contracte comporta obligacions essencials. L'entitat responsable de l'allotjament assumeix l'obligació de restitució de les dades. Com a dipositària, aquesta entitat assumeix l'obligació de no utilitzar les dades. No pot trencar el secret.*[26]

L'estatus d'entitat responsable de l'allotjament està regit per les disposicions d'ordre públic: l'entitat responsable de l'allotjament només pot rebre dades si ha estat admesa i està obligada pel secret professional. Així, el "dipositari natural" dels historials clínics i l'entitat responsable de l'allotjament estan subjectes a un mateix cos de regles d'ordre públic. Un decret precisa les condicions del consentiment i els controls exercits en relació amb les entitats responsables de l'allotjament de dades sobre la salut. El decret senyala sis condicions a complir per demanar el consentiment. Així, els contractes entre les entitats responsables de l'allotjament i clients han d'incloure clàusules obligatòries i aquestes entitats han d'elaborar i respectar una política de confidencialitat i seguretat.

Al Quebec, és la *Loi modifiant la Loi sur les services de santé et les services sociaux*[27] (Llei de modificació de la Llei sobre els serveis de salut i els serveis socials) la que introdueix un règim jurídic complet per als serveis regionals de conservació d'algunes dades per a la prestació de serveis sanitaris.

---

26 Vacarie, Isabelle, «L'hébergement des données de santé: entre contrat et statut», vol. 38 (4), R.D. *Sanit. Soc*, 2002, p. 695-698.

27 *Loi modifiant la Loi sur les services de santé et les services sociaux et d'autres dispositions législatives* (Llei de modificació de la Llei de serveis de salut i serveis socials i altres disposicions legislatives), L.Q., 2005, c. 32, art. 189.

Aquestes disposicions instituexen un Títol II intitulat "Serveis regionals de conservació d'algunes dades per a la prestació de serveis de salut"[28].

L'article 520.5 de la *Loi sur les services de santé et les services sociaux* (Llei sobre els serveis de salut i els serveis socials) enuncia finalitats-objectius que pretenen els serveis regionals de conservació de dades sobre la salut. Els objectius es precisen en l'article 520.5. Es tracta de proporcionar a les parts interessades habilitades la informació pertinent, organitzada, integrada i actualitzada per facilitar el coneixement ràpid de les dades sobre la salut d'una persona en el moment de fer-se càrrec o durant qualsevol prestació de serveis de salut proporcionats per aquestes parts interessades, en continuïtat i en complementarietat amb els proporcionats per altres parts interessades. L'altra finalitat mencionada en la Llei és assegurar l'eficàcia de la comunicació ulterior de les dades guardades per una agència o un establiment autoritzat a les parts interessades capacitades, amb l'única finalitat de prestació de serveis de salut.

La persona té dret d'accés a les dades que la concerneixen; pot demanar que les dades inexactes, incompletes o equívoques i les dades per a les quals la recopilació i comunicació no hagin estat autoritzades siguin rectificades. La Llei també organitza els recursos respecte a les entitats habilitades per assegurar la conservació de les dades. També s'afirma el principi de la responsabilitat i la imputabilitat de l'entitat autoritzada i de les altres entitats que asseguren el funcionament dels serveis de conservació. Per últim, les entitats responsables han de posar en marxa un conjunt de mecanismes per assegurar la disponibilitat, la integritat, la confidencialitat, l'accessibilitat i la irrevocabilitat de les dades que es posseeixen o es conserven. En alguns casos, és obligatori assegurar l'autenticació de la identitat de les persones habilitades.

Només les parts interessades habilitades tenen accés a les dades confiades als serveis regionals i únicament per a les finalitats estrictament delimitades. Aquests serveis de conservació només es poden aplicar mitjançant una autorització del ministre.

D'altra banda, s'apliquen condicions estrictes en relació a les mesures a prendre per assegurar la confidencialitat i la seguretat de les dades durant tot el seu cicle de vida. Tot accés a les dades s'ha d'enregistrar i els registres s'han de supervisar per poder detectar els accessos no autoritzats. S'han d'aplicar mecanismes de control intern per assegurar que les obligacions es respecten. Està prohibit confiar a un tercer la prestació de serveis de conservació, però és possible que un establiment autoritzat confiï a un tercer un contracte de servei relatiu a la instal·lació, manteniment o reparació de qualsevol suport tecnològic utilitzat per a les finalitats dels serveis de conservació.

---

[28] Trudel, Pierre, «Aperçu du cadre juridique des services d'hébergement de données de santé», en Barreau du Québec, *Après le projet 83: un nouveau réseau de la santé*, Formation continue, volum 260, Cowansville, Éditions Yvon Blais, 2006.

Qualsevol persona assegurada davant l'administració d'assegurances de malaltia, de més de catorze anys, pot donar el seu consentiment perquè les dades siguin bolcades als centres de conservació. Prèviament ha d'estar informada dels objectius i finalitats perseguits i de les modalitats de funcionament en relació a l'accés, la utilització, la comunicació, la conservació i la destrucció de les dades emmagatzemades. Se li ha d'especificar que el consentiment comporta l'autorització relativa a qualsevol part interessada habilitada a transmetre segons el seu perfil d'accés de recepció. Aquest consentiment és renovable. Es pot revocar en qualsevol moment a petició i ho és amb tot el dret quan una persona ja no està assegurada.

La revocació del consentiment segons els termes de l'article 520.23 comporta la desactivació de les dades conservades anteriorment. Aquestes dades no es poden destruir abans de cinc anys després de la seva inscripció. Està prohibit transmetre aquestes dades a una part interessada que no proporcioni a una persona serveis de salut o exerceixi respecte a una persona les funcions de control o de peritatge. També està prohibit transmetre les dades allotjades a un assegurador o a un patró i rebre extracte o còpia de les dades emmagatzemades. Es prohibeix que qualsevol persona tingui accés a aquestes dades, a un extracte o una còpia per a la conclusió de qualsevol contracte que exigeixi l'avaluació d'estat de salut d'una persona per a un contracte d'assegurança o d'ocupació o en qualsevol altre moment. Les dades conservades no es poden comunicar a cap persona, fins i tot amb el consentiment de l'interessat.

4.3. Els repertoris i els espais virtuals sota el control dels usuaris

El desenvolupament d'aplicacions a Internet que reserven a l'usuari un alt nivell de control sobre les informacions fa considerar nous modes de compartició de dades de caràcter personal. Efectivament, és possible posar en marxa espais personalitzats situats en part o totalment sota el control del ciutadà i que es puguin utilitzar en les interaccions d'aquest amb l'Administració. Uns espais informàtics d'aquestes característiques, situats sota el control de l'usuari, com una xarxa informàtica, li permeten situar els documents en un espai sota el seu control. Es distingeixen de la "finestra única" que són normalment llocs que federen serveis de procedència múltiple. La noció d'espai ciutadà ens remet més a espais virtuals en els quals està permès que l'usuari bolqui, conservi, autoritzi la consulta o la transmissió de dades amb la finalitat d'assegurar la realització de prestacions electròniques de serveis.

El model reflexa una tendència associada al que es denomina Web 2.0, basat (SOIT) en un gran control per part de l'usuari de la informació emmagatzemada i disponible a altres segons la seva elecció. El desenvolupament d'aquest tipus de contexts en línia que permeten intercanviar i compartir els documents tecnològics està recomanat pels qui volen assegurar la protecció dels documents en possessió de l'estat i pel ciutadà amb la finalitat de prestacions electròniques de servei. Per exemple, l'informe sobre l'administració electrònica *Vers un Québec branché pour ses citoyens* (Envers un Quebec connectat per

als ciutadans) ressalta la idea d'una "pàgina ciutadana"[29]. En aquest espai accessible en línia, el ciutadà podria tenir accés a les informacions que el concerneixen, consignar-hi els documents relatius a les relacions que estableix amb els diferents serveis i autoritzar la transmissió de documents requerits per a la realització de prestacions en línia.

Però ara per ara queda molt per fer per caracteritzar els diferents tipus d'espais en línia situats sota el control del ciutadà i que li permetin consignar documents tecnològics i, amb el seu consentiment, que estiguin disponibles per a altres entitats, especialment els ministeris i organismes públics en el context d'una prestació de servei.

Conclusió

A l'Estat en línia, les informacions són essencialment circulants, disponibles en el moment en què han d'estar-ho per tal de dur a terme una prestació de servei. Aquesta circulació necessita precaucions, ja que les potencialitats d'acumulació i d'acoblament de les informacions poden incrementar. Ara bé, l'adhesió d'una part de la població a algunes regles com ara les que prescriuen les exigències d'obtenir el "consentiment lliure i explícit" per a cada moviment d'informació personal sembla difícil de conciliar amb l'aplicació d'un marc jurídic que reflecteixi les característiques de les xarxes i per aquest motiu no hi hauria un marc jurídic que assegurés la protecció de la vida privada a l'Estat en xarxa.

La possessió en un context d'informació accessible a una pluralitat d'organismes públics, per permetre'ls assegurar per si mateixos o en cooperació un conjunt de serveis als ciutadans, només és factible si existeixen fortes mesures per garantir la protecció de la vida privada. La formulació d'un marc jurídic d'aquestes característiques suposa una lectura actualitzada dels principis fonamentals de la protecció de les dades de caràcter personal. Una protecció situada al nivell dels accessos per les administracions procura una protecció molt superior a la que podem esperar dels règims actuals que es deriven de les lleis relatives a la protecció de dades personals.

La connexió en xarxa de les dades administratives apunta a una relectura dels principis de protecció per assegurar una gestió plenament compatible amb les exigències, riscs i desafiaments que plantegen les xarxes i les exigències de la protecció efectiva dels drets de les persones. Per tenir en compte els desafiaments en relació amb la protecció de les informacions personals, és necessari mirar amb lucidesa els riscs que es deriven del caràcter confidencial de les dades i del context inherent a la xarxa. Els mecanismes jurídics han de procurar la protecció efectiva sense obstaculitzar la circulació de la informació que és inherent a la posada en marxa dels serveis en xarxa.

---

29 Gautrin, Henri-François, *Rapport sur le gouvernement en ligne, vers un Québec branché pour ses citoyens*, Quebec, juny 2004, p. 49.

Els models emergents per formular els marcs dels usos compartits de les dades de caràcter personal mostren les vies que extrau l'adaptació del dret als imperatius de la virtualització. Podem veure l'aspecte que pren la modernització dels mecanismes de protecció –fundats sobre el paradigma dels dossiers en paper substituint-los en un marc que assegura tant la mobilitat com la confidencialitat de la informació. També es compaginen les noves exigències relatives a la qualitat de la informació requerida per assegurar els serveis públics.

Els marcs jurídics que tendiran a implantar-se a l'Estat en xarxa han de garantir tant la plena disponibilitat de les dades a tots els que han de tenir-hi accés com la protecció en relació a les altres utilitzacions. Tot això posa de manifest que la implantació de models innovadors de compartició de dades personals constitueix un desafiament major del desplegament dels serveis en línia i de la modernització dels serveis públics.