ADMINISTRACIÓN ELECTRÓNICA E INTERCONEXIÓN DE FICHEROS ADMINISTRATIVOS EN EL ESTADO EN RED

Pierre Trudel[*]

Sumario

1. Los imperativos de la Administración electrónica
2. Los imperativos de la protección de la vida privada y los datos de carácter personal
3. La compartición de los datos de carácter personal entre las administraciones
   - 3.1. La comunicación efectuada con el consentimiento del interesado
   - 3.2. Las habilitaciones generales para compartir las informaciones personales
   - 3.3. Los acuerdos de compartición
4. El modelo de red para explicar la protección de los derechos en los servicios transgubernamentales
   - 4.1. Las áreas de compartición de los datos de carácter personal
   - 4.2. Los repertorios de informaciones personales sobre la salud disponibles en línea con el consentimiento del paciente
   - 4.3. Los repertorios y los espacios virtuales bajo el control de los usuarios

Conclusión

[*] Pierre Trudel, profesor titular de la Cátedra L. R. Wilson sobre Derecho de las Tecnologías de la Información y el Comercio Electrónico <chairelrwilson.net>, Centro de Investigación de Derecho Público, Facultad de Derecho, Universidad de Montreal, <pierre.trudel@umontreal.ca>.

Artículo recibido el 31.05.2007

La mutación del Estado deriva particularmente del acceso a las tecnologías en red. El inicio de la Administración electrónica es característico de las mutaciones inducidas en el derecho los recursos a las tecnologías de la información para asegurar el funcionamiento de los servicios gubernamentales. El universo posmoderno característico de los países afectados por la revolución digital se refleja en la morfología del derecho.[1] Como consecuencia, se deriva una redefinición de las condiciones de la intervención jurídica y las formas de concebir el derecho. Una redefinición de estas características concierne en primer lugar las prácticas relativas a la protección de los datos de carácter personal que están en posesión de la Administración.

Este estudio se ha llevado a cabo desde la perspectiva canadiense. Canadá es un Estado federal. Los textos constitucionales dividen la totalidad de los poderes de aprobar leyes entre el Parlamento federal y las legislaturas de las provincias.[2] Según la tradición del gobierno parlamentario británico introducida en el Canadá en el siglo XVIII, los ministerios son responsables de los documentos y de la información que están en su posesión. El acceso a los servicios en línea presenta un reto adicional: asegurar los servicios integrados con respecto a las materias que pueden depender de la competencia de entidades que pertenecen a niveles múltiples de gobierno.

Desde el punto de vista de los ciudadanos y los administrados, las interacciones con las instancias estatales que dependen del Parlamento federal y de las legislaturas provinciales suponen múltiples intercambios de información. Por ejemplo, para obtener un pasaporte, el ciudadano canadiense tiene que presentar la información necesaria para acreditar su ciudadanía. Para hacerlo, tendrá que presentar un documento del estado civil que suelen emitir las autoridades que dependen de las provincias. Éste es sólo un ejemplo de las diversas situaciones en las cuales están implicadas una pluralidad de instancias gubernamentales dependientes del Estado federal o de una provincia. En sus campos respectivos de competencias, las provincias y el Parlamento federal han aprobado leyes relativas a la protección de los datos de carácter personal. La protección de los datos personales está regida por textos que distinguen entre el sector privado y el sector público. Los mecanismos de protección mínimos están dictados en los textos relativos al sector privado. De las leyes se derivan protecciones reforzadas que se aplican a las entidades que dependen del Estado o del sector público.

Para poder explicar los marcos jurídicos relativos a la interconexión de ficheros administrativos en el Estado en red, en primer lugar es importante recordar los imperativos de la administración electrónica. Después se tomarán en cuenta las exigencias relativas a la protección de datos de carácter personal y se presentará el régimen jurídico de los intercambios de datos previsto por las leyes sobre la protección de datos de carácter personal. Por último se presentarán los modelos emergentes de mecanismos jurídicos destinados a asegurar la compartición etiquetada de los datos personales entre una pluralidad de entidades del Estado.

---

1 Chevalier, Jacques, *La État post-moderne*, 2ª edición, París LGDJ, 2004; Morand, Charles-Albert, *Le droit néo-moderne desde politiques publicas*, París LGDJ, 2000.

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

1. Los imperativos de la Administración electrónica

Los puntos clave que marcan el desarrollo del derecho relativo a la administración electrónica se basan en el ajuste de los principios jurídicos con el objetivo de enmarcar las interacciones en línea. El marco jurídico de la administración electrónica está marcado por las visiones de gestión del Estado.[3] Las políticas de implantación de la administración electrónica o de "la administración en directo" se conciben según una lógica de reconfiguración de la oferta de servicios del Estado en función de una aproximación basada en el ciudadano considerado como un "cliente".

Kenneth Kernaghan y Justin Gunraj sostienen que el incremento en la adopción de las tecnologías de la información por parte de las administraciones gubernamentales predispone a los organismos públicos a cambiar sus estructuras y sus formas de gestión.[4] Un primer factor de cambio introducido por las tecnologías de la información es la presión engendrada por las fuertes inversiones y el consiguiente movimiento hacia una cooperación más intensiva entre los organismos gubernamentales. Un segundo factor insiste en la necesidad creciente de evaluación y de capacidades mayores de compartir la información. Todo eso lleva a la creación de entidades no ministeriales. De esta manera, en Canadá se han creado unas "agencias" que se presentan como estructuras con características más adaptadas al de funciones horizontales. Un tercer factor de cambio sería el desplazamiento de una parte del nivel intermediario de gestión en beneficio de una cierta horizontalidad de la jerarquía administrativa, la autoridad y los controles. Junto con la acentuación de las posibilidades de diálogo directo con los administrados, este factor comporta el replanteamiento de los enfoques sobre los cuales se fundamentan los mecanismos de protección de datos de carácter personal en posesión de la Administración gubernamental.

Las interconexiones son un componente destacable del Estado en red. Los intercambios de información son constantes y no se puede suponer que estos intercambios se dan en un espacio territorial u organizativo determinado. Por ejemplo, el funcionamiento de la mayor parte de los servicios en línea se basa en el hipertexto. Eso permite y generaliza las posibilidades de intercreatividad, de interrelaciones y de intercambio de informaciones. A partir de ahora las informaciones están tanto aquí como en otro lugar al mismo tiempo, incluso en una o en diversas pantallas de ordenador, de televisión, de radios digitales o de teléfonos móviles. Un entorno de estas características supone una compartición mayor de informaciones, pero etiquetadas.

La generalización de las plataformas de compartición de información pone al alcance de los usuarios y de las administraciones un conjunto de posibilidades de intercambio de informaciones. Los internautas, los ciudadanos gestores y los agentes del Estado pueden comunicar, compartir e intercambiar

---

3 Chevallier, Jacques, «La juridicisation desde préceptes managériaux», quiere. 11, *Politique te management public*, 1993, p. 111-134.

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

información. Teniendo en cuenta este contexto, el marco jurídico relativo a la información que está necesariamente en posesión de la Administración tendría que regir las condiciones de acceso de cada agente del Estado más que prohibir la circulación. En un Estado en red, la cuestión no es tanto saber si una información puede estar o no en posesión de la Administración, sino si la Administración tiene el derecho de acceder y de usarla para tomar una decisión en una situación concreta.

Las interacciones en el contexto de las redes informáticas requieren modalidades diferentes de gestión de la información. Las administraciones funcionan cada vez más siguiendo una lógica de red y las informaciones son principalmente circulantes, disponibles en el momento en que tienen que estarlo para cumplir una prestación de servicio. Las condiciones de circulación creciente de las informaciones también necesitan que se tomen precauciones, ya que las posibilidades de acumulación y de acoplamiento de la información son cada vez más considerables. Esta situación nos invita a una actitud realista y a tener en cuenta tanto las ventajas de la circulación de la información como los inconvenientes.

2. Los imperativos de la protección de la vida privada y los datos de carácter personal

La protección de la vida privada y de los datos de carácter personal se identifica normalmente como una de las cuestiones más importantes del desarrollo de la administración electrónica. En el ámbito federal, la *Loi sur la protection de renseignements personnels* (Ley de protección de datos de carácter personal), que entró en vigor el 1 de julio de 1983, gestiona la protección de los datos de carácter personal en el sector público federal.[5] Esta ley persigue el doble objetivo de proteger los datos personales[6] mediante la limitación de la recopilación, utilización y comunicación de datos, y asegurar el derecho de acceso y corrección de los individuos a los datos personales que les conciernen[7] que están en posesión de las organizaciones federales. Por lo tanto, se aplica en las instituciones federales, es decir, en cualquier

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

6 La expresión *datos personales*, definida al artículo 3 de la ley, se interpreta de la siguiente manera en *Dagg c. Canada (Ministre des Finances*), [1995] 3 C.F. 199 (C.A.) y en *Canada (Commissaire à l'information) c. Canada (Commissaire de la Gendarmerie royale du Canada*), [2003] 1 R.C.S. 66: por *datos personales* se entiende cualquier información sobre un individuo identificable relativa a sus características personales, educación, historial médico, antecedentes penales, cualquier número o símbolo u otra indicación identificativa, dirección, huellas digitales, grupo sanguíneo, opiniones o ideas personales, cualquier correspondencia de carácter implícitamente o explícitamente privado o confidencial, ideas u opiniones de otros sobre él, su apellido cuando se menciona con otros datos sobre él o cuando la simple divulgación de su apellido revelara datos sobre su persona. En la ley quebequesa la noción de *datos personales* tiene un espectro muy amplio. El artículo 54 indica que "en un documento son personales los datos que conciernen a una persona física y permiten identificarla" y son datos considerados por ley "confidenciales a no ser que su divulgación esté autorizada por la persona interesada".

7 Estos dos objetivos están establecidos en las siguientes decisiones: *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.

ministerio o departamento del Estado que depende del Gobierno de Canadá o cualquier organismo incluido en el anexo de la ley, lo que representa unos 150 ministerios y organismos federales.

Las provincias y los territorios también han adoptado leyes sobre la protección de los datos personales.[8] Del mismo modo que la legislación federal, estas leyes rigen la recopilación, la utilización y la comunicación de los datos de carácter personal en posesión de los organismos dependientes tanto de los gobiernos provinciales como locales. Confieren a las personas el derecho a solicitar el acceso a sus datos personales y a rectificarlos cuando sea necesario. La vigilancia de la aplicación de estas leyes está generalmente asegurada por un comisario, un *ombudsman* o una comisión independiente que tiene el poder de recibir quejas y llevar a cabo investigaciones[9].

De estos textos legislativos, tanto en el ámbito federal como en el provincial, se desprenden diversos principios relativos al consentimiento, la limitación de la recopilación, la utilización y la comunicación de datos de carácter personal, los derechos de acceso y de corrección de los interesados por los datos y, por último, al ejercicio de un recurso independiente.

Las excepciones al principio de confidencialidad de los datos de carácter personal están limitadas a los casos en que los datos son necesarios para luchar contra el crimen, a las situaciones de urgencia en que la seguridad o la vida del interesado estén en peligro y con propósitos de estudio o de investigación. Las otras excepciones importantes a la confidencialidad de los datos de carácter personal son las relacionadas con los acuerdos de transferencia de estos datos entre organismos. Son estos mecanismos los que parecen tener la intención de evolucionar para reflejar los imperativos del Estado en red.

---

8 Los principales textos de cada provincia y territorio son: **Quebec**: *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (L.R.Q., c. A-2.1); **Ontario**: *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; **Columbia Británica:** *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; **Isla del Príncipe Eduardo**: Freedom of Information and Protection of Privacy Act, S.P.E. I. 2001, c. 37; **New Brunsvic**: *Protection of personal Information Act*, S.N.B. 1998, c. P-19.1; **Nueva Escocia**: *Freedom of Information and Protection of Privacy Act*, S.N.S. 1993, c. 5; **Terranova y 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; **Territorios del Noroeste**: *Access to Information and Protection of Privacy Act*, S.N.W.T. 1994, c. 20.

9 Para obtener una descripción del conjunto de las leyes canadienses sobre la protección de los datos de carácter personal, se puede consultar McIsaac, Barbara; Rick Shields i Kris Klein, *The law of privacy in Canada*, looseleaf edition, vol. 1, Scarborough (Ontàrio), Thomson/Carswell, 2000.

3. La compartición de los datos de carácter personal entre las administraciones

Las legislaciones relativas a la protección de datos de carácter personal en posesión de las autoridades gubernamentales consagran el principio según el cual cada organismo público es una entidad autónoma y responsable de la protección de los datos personal que tiene en su posesión.[10] A la luz de la experiencia de la aplicación de las leyes de protección de datos de carácter personal, está comprobado que las disposiciones que prevén la posibilidad de que un organismo comparta algunas informaciones personales respetando las condiciones pronunciadas son necesarias para el funcionamiento adecuado de los servicios públicos. Esta necesidad es especialmente evidente cuando se trata de asegurar la prestación en línea de servicios personalizados al ciudadano.

La circulación de los datos de carácter personal entre las entidades gubernamentales está regida bien por las disposiciones de la ley que permiten la transmisión con las condiciones que allí precisa, bien por los acuerdos o bien por la regla del consentimiento explícito de la persona concernida por los datos.

Se prevén tres mecanismos para enmarcar la compartición de datos personales entre las entidades gubernamentales. Evidentemente, el interesado también puede autorizar esta comunicación. No obstante, hay habilitaciones previstas expresamente por las leyes en virtud de las cuales los datos de carácter personal se pueden comunicar a otras administraciones. Un conjunto de reglas enmarcan los acuerdos de compartición de datos de carácter personal entre las entidades gubernamentales.

3.1. La comunicación efectuada con el consentimiento del interesado

El consentimiento es la manifestación de la voluntad de una persona de suscribir un acto jurídico. Con respecto a los datos de carácter personal, el consentimiento comprende el uso que se puede hacer. El consentimiento es necesario para autorizar el uso de los datos de carácter personal durante las diferentes etapas de su ciclo de vida. Para que sea válido, el consentimiento tiene que ser manifiesto, libre y explícito, para finalidades específicas, por una duración determinada y expresado por el interesado.

Para que sea válido, el consentimiento lo tiene que dar el interesado. El interesado tiene que ser capaz, es decir, tiene que tener la facultad de ser titular de los derechos y de ejercerlos por sí mismo. No obstante, teniendo en cuenta las consecuencias de la edad y del deterioro del estado físico o mental del interesado, se han previsto medidas de protección para garantizar los intereses de los menores y de algunos mayores. En este caso, el consentimiento lo dan terceras personas. Evidentemente, el consentimiento se puede solicitar y dar en línea. Por otra parte, una de las ventajas más prometedoras asociada a las prestaciones electrónicas de los servicios públicos es la mayor capacidad de diálogo entre el ciudadano-usuario y la Administración durante las interacciones en línea.

---

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

El consentimiento tiene que ser libre y explícito. Eso significa que tiene que darse sin ninguna coacción y con conocimiento de causa. Por lo tanto, la entidad que recoge los datos de carácter personal tiene la obligación de informar al interesado de todos los hechos pertinentes relativos a las actividades para las cuales se solicita su acuerdo. La exigencia del carácter manifiesto significa que el consentimiento se puede dar verbalmente o por escrito, a condición de que sea evidente y claro que la persona ha consentido en el uso o la divulgación de información.[11]

El consentimiento se da para finalidades específicas y por una duración limitada. Una vez que el propósito se ha cumplido, ya no se deberían utilizar los datos personales, excepto para obtener un nuevo consentimiento del interesado o de cualquier otra persona autorizada por ley. El mismo criterio se aplica si el poseedor de los datos de carácter personal quiere utilizarlas para otra finalidad diferente a la prevista inicialmente.

No obstante, hay excepciones a esta exigencia de consentimiento para la transferencia o comunicación de datos de carácter personal. Una disposición legislativa o la orden de un tribunal pueden permitir la divulgación o la transferencia de datos de carácter personal sin necesidad de consentimiento.

3.2. Las habilitaciones generales para compartir las informaciones personales

Los organismos públicos están capacitados por ley para compartir datos de carácter personal cuando estos datos son necesarios para luchar contra el crimen[12] o en situaciones de urgencia donde la seguridad o la vida del interesado estén en peligro.

Las disposiciones prevén que un organismo público pueda comunicar, a cualquier persona o a otro organismo público, una información nominativa sin el acuerdo del interesado si esta divulgación es necesaria para la aplicación de una ley. Esta disposición está formulada de la siguiente manera:

> ***67.*** *Un organismo público puede, sin el consentimiento del interesado, comunicar información nominativa a cualquier persona u organismo si esta comunicación es necesaria para la aplicación de una ley en Quebec, tanto si esta comunicación está prevista expresamente por la ley como si no lo está.*

Desde el día siguiente a la entrada en vigor de la Ley, la Comisión de acceso ha mostrado una tendencia para mantener una interpretación restrictiva de la noción de necesidad para la aplicación de una

---

11 La *Loi sur la protection des renseignements personnels et les documents électroniques* [Ley de protección de datos de carácter personal y documentos electrónicos] en el artículo 4.3.7 del anexo prevé que el consentimiento, necesario desde la recopilación de los datos personales, puede revestir diferentes formas, teniendo en cuenta que según el artículo 4.3.4 del anexo "la forma del consentimiento que el organismo quiere obtener puede variar según las circunstancias y el carácter de los datos". De esta manera, el consentimiento tendrá que ser explícito si los datos son considerados confidenciales. Normalmente, un consentimiento implícito será suficiente si los datos son considerados menos confidenciales. La ley precisa, sin embargo, que todos los datos se pueden convertir en confidenciales después de la recopilación. Parece, pues, que la apreciación del grado de confidencialidad de los datos se deje a los organismos que los recopilan.

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.

ley. Aunque sea necesario demostrar que la comunicación de estos datos es "indispensable, esencial y primordial". Doray y Charrette recuerdan que según esta estricta interpretación "[...] es esencial que una ley mencione expresamente que un organismo público tiene que comunicar las informaciones nominativas a una persona o a un organismo público o privado para que el artículo 67 se pueda aplicar".[13] Las enmiendas introducidas el año 2006 terminaron con esta tendencia al precisar que no es necesario que la comunicación esté prevista expresamente por ley.

Entre las excepciones previstas del carácter confidencial de los datos personales, existen las disposiciones que autorizan la comunicación a un organismo de otro gobierno. El párrafo 68(1°) de la ley quebequesa indica que un organismo público puede comunicar información personal "a un organismo de otro gobierno si esta comunicación es necesaria para el ejercicio de las atribuciones del organismo receptor o para poner en funcionamiento un programa gestionado por este organismo".

El párrafo 68(1.1°) prevé que un organismo público pueda comunicar información personal "a un organismo de otro gobierno si esta comunicación es inequívocamente en beneficio de la persona interesada". Igualmente, el párrafo 68(3°) autoriza la comunicación de información personal:

> *a una persona o a un organismo si esta comunicación es necesaria en el contexto de la prestación de un servicio a la persona interesada por parte de un organismo público, especialmente con el objetivo de identificar a esta persona.*

Por lo que respecta a las comunicaciones en el exterior del Quebec, "el organismo público tiene que asegurarse de que tendrán una protección equivalente a la prevista en la presente ley".[14] Si el organismo público estima que las informaciones privadas "no tendrán una protección equivalente a la prevista en la presente ley, tiene que negarse a comunicarlas o negarse a confiar a una persona u organismo en el exterior de Quebec la tarea de gestionarlas, utilizarlas o comunicarlas por su cuenta".[15]

3.3. Los acuerdos de compartición

Las condiciones de compartición de datos están normalmente regidas por acuerdos entre los organismos implicados. Sólo la ley quebequesa especifica los elementos que tienen que figurar en los acuerdos. Para que los acuerdos puedan intervenir entre el gobierno de Canadá y el gobierno de una de las provincias, el Secrétariat du Conseil du Trésor ha emitido unas directrices para los ministerios y organismos federales sobre los elementos que tienen que contener estos acuerdos.[16] Los acuerdos de intercambio de datos personales deben incluir:

---

13 Raymond Doray y 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* (Ley de acceso a los documentos de los organismos públicos y la protección de datos de carácter 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*, (Ley de acceso a los documentos de los organismos públicos y la protección de datos de carácter personal) (L.R.Q. A-2.1).

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

- una descripción de los datos de carácter personal que se compartirán;
- los objetivos por los cuales los datos se comparten y se utilizan;
- un enunciado de todas las medidas de protección administrativas, técnicas y materiales necesarias para la protección del carácter confidencial de los datos, sobre todo en lo que concierne a su uso y comunicación;
- un enunciado que precise si los datos recibidos por la institución federal estarán sujetos a las disposiciones de la Ley de protección de datos de carácter personal (por ejemplo, si los interesados pueden tener acceso a los datos y, si no, qué excepciones se recomiendan para la institución que proporciona los datos);
- un enunciado que precise si los datos comunicados por la institución federal estarán sujetos a las disposiciones de la Ley de protección de datos de carácter personal (por ejemplo, si la institución que recibe los datos puede dar acceso a los interesados y, si no, qué excepciones se recomiendan);
- un enunciado que indique que la compartición de datos terminará si el beneficiario comunica de manera inoportuna los datos de carácter personal compartidos;
- el nombre, el título y la firma del agente autorizado de la institución que proporciona los datos de carácter personal y de la que los recibe, así como la fecha del acuerdo.

En el Quebec, el régimen de acuerdos de compartición de datos de carácter personal está definido más concretamente en los artículos 67 y posteriores de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Ley sobre el acceso a los documentos de los organismos públicos y sobre la protección de los datos personales). La transmisión de informaciones personales tiene que estar enmarcada por acuerdos con las finalidades del cumplimiento de un mandato. Los artículos 67.2 y 67.3 prevén que un organismo público puede, sin el consentimiento del interesado, comunicar información nominativa a cualquier persona u organismo si esta comunicación es necesaria para el ejercicio de un mandato confiado por el organismo público a esta persona u organismo. En este caso, el organismo público, en primer lugar, ha de confiar este mandato por escrito y, en segundo lugar, consignar un conjunto de indicaciones. El organismo tiene que indicar, en este mandato, las disposiciones de la ley que se aplican a la información que ha sido comunicada así como las medidas que se tienen que tomar para que esta información no se utilice en el ejercicio del mandato. Se debe precisar que los datos de carácter personal serán destruidos después de la expiración del mandato. Además, el organismo público tiene que obtener, antes de la comunicación, un compromiso de confidencialidad cumplimentado por todas las personas a quienes se pueden comunicar los datos, excepto si el responsable de la protección de los datos de carácter personal estima que no es necesario. Una persona o un organismo que ejerce un mandato o ejecuta un contrato de servicio incluido en el primer párrafo tiene que informar sin dilación al responsable de cualquier infracción o tentativa de infracción por cualquier persona de las obligaciones relativas a la confidencialidad de los datos comunicados y también debe permitir que el responsable efectúe cualquier verificación relativa a esta confidencialidad.

El registro de los acuerdos de compartición de informaciones personales comprenden precisión sobre:

1 *la naturaleza o el tipo de datos comunicados;*
2 *la persona o el organismo que recibe esta comunicación;*
3 *la finalidad con la cual se comunican estos datos y la indicación, si es necesario, de que se trata de una comunicación incluida en el artículo 70.1;*
4 *la razón que justifica esta comunicación;*

En el caso de un acuerdo sobre la recopilación de datos personales, el registro comprende:

1 *el nombre del organismo para el cual se recopilan los datos;*
2 *la identificación del programa o de la atribución para el cual los datos son necesarios;*
3 *la naturaleza o el tipo de prestación de servicio o de misión;*
4 *la naturaleza o el tipo de datos recopilados;*
5 *la finalidad con la cual se recopilan los datos;*
6 *la categoría de personas, en el seno del organismo que recoge los datos y en el seno del organismo que los recibe, que tienen acceso a los datos.*

En el caso de la utilización de datos de carácter personal con una finalidad diferente a la finalidad con que se recopilaron, el registro comprende:

1 *la mención del apartado del segundo párrafo del artículo 65.1 que permite su utilización;*
2 *en el caso previsto en el apartado 3 del segundo párrafo del artículo 65.1, la disposición de la ley que hace necesaria la utilización de los datos;*
3 *la categoría de personas que tienen acceso a los datos con la finalidad de la utilización indicada.*

El registro es accesible a toda persona que lo solicite, excepto en relación con los datos de carácter personal, la confirmación de la existencia de los cuales puede ser rechazada en virtud de las disposiciones de la ley que protegen los datos en posesión de las fuerzas policíacas (art. 67.4).

Como hemos señalado, las disposiciones autorizan la comunicación de datos de carácter personal en un organismo de otro gobierno. Así, el párrafo 68(1°) indica que un organismo público puede comunicar información personal "a un organismo de otro gobierno si esta comunicación es necesaria para el ejercicio de las atribuciones del organismo receptor o el funcionamiento de un programa gestionado por este organismo". Con el mismo carácter, el párrafo 68(1.1°) prevé que un organismo público pueda comunicar información personal "a un organismo de otro gobierno si la comunicación es inequívocamente en beneficio del interesado". Recordemos también que el párrafo 68(3°) autoriza la comunicación de información de carácter personal "en una persona o un organismo si esta comunicación es necesaria en el contexto de la prestación de un servicio a la persona interesada por parte de un organismo público, especialmente con el objetivo de identificar a esta persona".

En los tres casos mencionados anteriormente, la comunicación se efectúa en el contexto de un acuerdo escrito. Este acuerdo se tiene que someter a la Comisión para su dictamen.[17] Cuándo tiene que emitir un dictamen en relación con un acuerdo de compartición de datos de carácter personal, la Comisión debe tomar en consideración la conformidad del acuerdo con las condiciones incluidas en el artículo 68 o en el artículo 68.1, es decir, que el intercambio se refiere a una situación donde la comunicación es necesaria para el ejercicio de las atribuciones del organismo receptor o el funcionamiento de un programa gestionado por este organismo. En otras situaciones, habrá que asegurar que la comunicación es en beneficio de la persona interesada o que es necesaria para la aplicación de una ley.

La Ley también pide que la Comisión considere el impacto de la comunicación de los datos en la vida privada del interesado, si es necesario, en relación con la necesidad del organismo o la persona que recibe la comunicación de tener estos datos.

La Comisión debe emitir un dictamen motivado en un plazo máximo de 60 días a partir de la recepción de la petición de dictamen acompañada del acuerdo. Si la petición se modifica durante el plazo, éste empieza a contar desde la última petición. Si no es posible la tramitación de la petición de dictamen en este plazo sin perjudicar el desarrollo normal de las actividades de la Comisión, el presidente puede, antes de la expiración del plazo, prolongarlo por un periodo máximo de 20 días. Tiene que informar a las partes del acuerdo en el plazo de 60 días.

El acuerdo entra en vigor con el dictamen favorable de la Comisión o en la fecha posterior prevista en el acuerdo. La Comisión tiene que hacer público este acuerdo y su dictamen. Si no hay dictamen en el plazo previsto, las partes del acuerdo están autorizadas a proceder con su ejecución.

En caso de dictamen desfavorable de la Comisión, el gobierno puede, a petición, aprobar el acuerdo y fijar las condiciones aplicables. Antes de aprobar el acuerdo, el gobierno publica en la *Gazette officielle du Québec* el acuerdo y, si es necesario, las condiciones que prevé fijar con un dictamen que podrá aprobar el acuerdo cuando expire el plazo de 30 días de esta publicación y que toda persona interesada puede, durante este plazo, transmitir comentarios a la persona designada. El acuerdo entra en vigor el día de su aprobación o en la fecha posterior fijada por el gobierno o prevista en el acuerdo. Este acuerdo, el dictamen de la Comisión y la aprobación del gobierno se presentan a la Asamblea nacional durante los 30 días posteriores a la aprobación si la Asamblea está en sesión o, si no está reunida, en los 30 días posteriores a la reanudación del trabajo. El gobierno puede revocar en cualquier momento un acuerdo de estas características.[18]

Aunque tengan derecho de acceso a los registros que recopilan los acuerdos de intercambio de datos de carácter personal, los ciudadanos no están informados sistemáticamente de las consecuencias que estos acuerdos pueden tener sobre la comunicación secundaria de datos personales que deben

---

17 Art. 70, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (Ley de acceso a los documentos de los organismos públicos y la protección de datos de carácter personal) (L.R.Q. A-2.1).

18 Art. 70, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Ley de acceso a los documentos de los organismos públicos y la protección de datos de carácter personal) (L.R.Q. A-2.1).

proporcionar. No hay un proceso público de evaluación que permita apreciar los impactos, los riesgos y los desafíos que estos intercambios pueden comportar.

Cuando las transmisiones se autorizan, comportan la posibilidad de que el organismo público receptor se convierta en el poseedor de la totalidad de los datos concernidos. Por ejemplo en el Quebec, donde existen disposiciones más detalladas, el proceso de aprobación por la Comisión, cuando ocurre, no está precedido de un debate público y controvertido. La Comisión recibe una petición y emite un dictamen normalmente a partir de la información proporcionada por el ministerio u organismo pertinente. No hay audiencia pública en la cual el organismo público y los interesados puedan debatir los desafíos y los riesgos.

4. El modelo de red para explicar la protección de los derechos en los servicios transgubernamentales

Desde el punto de vista del ciudadano, el Estado se presenta cada vez más como una red en la cual las fronteras administrativas parecen tener cada vez menos pertinencia. Este fenómeno favorece un incremento de las responsabilidades reguladoras de los actores en primera línea y aumenta la necesidad de desarrollar instrumentos para asegurar el desarrollo de instrumentos reguladores apropiados a nivel local y de los microcentros virtuales.

La red sustituye cada vez más las instituciones jerarquizadas como lugar de concepción y de enunciación de la normatividad. De aquí la idea de una regulación relevada en diversos vectores. Esta tendencia hace pensar que las instituciones habituadas a modelos flexibles de regulación son las más susceptibles de actuar con eficacia en el universo digital del Estado en línea.

La red supone la emergencia de espacios interconectados que vinculan responsables, investigadores y reguladores así como a otros actores que tienen un papel en el gobierno de los espacios en el seno de los cuales discurren las actividades del gobierno.[19] Es lo que encontramos en los espacios de interacción entre la Administración y los ciudadanos. En su "modelo integrado de administración electrónica", Réjean Roy incluye la dimensión jurídica en el número de elementos del marco común del gobierno de la administración electrónica.[20] Las normatividades jurídicas contribuyen con las normatividades administrativas, tecnológicas y políticas a enmarcar las interacciones y los intercambios de información en el seno del aparato gubernamental.

Este tipo de modelo rinde cuentas de la dimensión en red de la administración electrónica, del hecho de que el espacio que nos ocupa es un conjunto interconectado constituido por polos que interactúan

---

19 Castells, Manuel, *La société en réseaux. L'ère de l'information*, Paris, Fayard, 1998; François Ost y Michel de KERCHOVE, *De la pyramide au réseau: pour une théorie dialectique du droit*, Bruselas, 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>.

con normatividades. Está constituido por espacios en los cuales prevalecen completamente o parcialmente normas que se imponen a los usuarios y otros socios. Las normas pueden imponerse bien por su capacidad de definir, incluso implícitamente, las condiciones del ejercicio de las actividades, o bien porque un participante está en condiciones de ejercer una autoridad. Este espacio también está constituido por relevos por los cuales se explicitan y se difunden tanto las normatividades como sus consecuencias. Las reglas que emanan de los polos de normatividad se relevan y se difunden a los diferentes espacios virtuales. Coexisten bien en complementariedad con otras reglas o bien en competencia, cuando se proponen en lugar de las reglas que han surgido de otros polos normativos.[21]

La normatividad en red característica de los espacios fundados en el uso de las redes de comunicación informática comporta cambios en las maneras de concebir el reparto de las responsabilidades.[22] El modelo clásico, característico del Estado liberal donde cada ministerio o entidad administrativa se considera que tiene el control completo y exclusivo de sus datos, está gradualmente cambiando a un modelo donde la compartición de información exige aplicar nuevas formas de distribución y reparto de responsabilidades.

Si en el universo burocrático dominado por el papel el derecho insiste en la delimitación de los derechos de obtener o no una información u otra, en el universo en red el derecho tiende a la organización de una regulación de permisos de acceso y de uso correspondientes a los responsables y a los ciudadanos.

Parece que se perfila una tendencia hacia una evolución de las concepciones que velan por la interpretación de los principios fundamentales relativos a la gestión de los datos personales. Así, la limitación en materia de recopilación supone poner en funcionamiento procesos de decisión que utilizarán la mínima información necesaria para asegurar las prestaciones o la toma de decisiones. Es necesario poder justificar el porqué de la recopilación de cada información personal.

En un contexto en red, la necesidad de la recopilación se tiene que contemplar en relación con el conjunto de familias de prestaciones concernidas por las informaciones. Cuando la información se ha recopilado, la necesidad de su conservación se puede apreciar en relación con un conjunto de procesos de decisión susceptibles de realizarse recurriendo a una información personal. El principio de retención en materia de recopilada y el principio de especificación de las finalidades coinciden. El principio relativo a la especificación de las finalidades también está reforzado: al especificar lo más tajantemente posible las finalidades, estaremos en una situación en la cual la recopilación estará limitada a las informaciones efectivamente indispensables, a las finalidades perseguidas por el plan del conjunto de las prestaciones y servicios que tendrán que estar asegurados en el seno de una red.

---

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 las mutaciones del modelo piramidal hacia un derecho en red, véase: Bailleux, Antoine, «À la recherche des formes du droit: de la pyramide au réseau», vol. 55, RIEJ, 2005, p. 91-115.

La regla que impide la circulación y la reutilización de la información porque esta información se podría desviar de su finalidad se tiene que situar en el contexto de mayor diálogo que permite la red. Más que nunca, la Administración está en condiciones de indicar a cada administrado qué información tiene, qué información pretende utilizar para tomar una decisión. El ciudadano está de ahora adelante en posición de interactuar y de exigir que se retire o se añada información.

La generalización de las redes lleva a reconocer la necesidad con respecto al conjunto de las situaciones concernidas por un contexto de información. En efecto, siempre se tiene que considerar la necesidad en el plan de la legitimidad de la recopilación y de la posesión de información, como exigen los principios actuales. Pero también se tiene que asegurar de que sólo la información pertinente y autorizada se utiliza en el marco de un proceso de decisión específico. Se necesita, pues, una gestión en que se disocian, por una parte, la cuestión de la necesidad de la posesión de la información y, por otra parte, la apreciación de la necesidad de acceder por una decisión o prestación determinada.

El principio de finalidad implica que sólo se pueden recopilar y utilizar datos de carácter personal para finalidades compatibles con las de la recopilación inicial. El principio de finalidad está ligado al mantenimiento de la calidad de la información. En los principios de la OCDE, esta exigencia se explica así:

> *Los datos de carácter personal tienen que ser pertinentes en relación con las finalidades para las cuales se tendrán que utilizar y, en la medida en que estas finalidades lo exijan, tendrán que ser exactas, completas y actualizadas.*[23]

En el contexto de un espacio en red, la cuestión de la finalidad se plantea teniendo en cuenta que la información puede estar allí disponible, ya recopilada: la exigencia de respetar la finalidad ya no se aplica tanto a la posesión sino al acceso y a la utilización de los datos. En una red, el principio de control del derecho de acceso asegura que se respeta la finalidad. El acceso a una información sólo es lícito para una finalidad autorizada y si se realiza una actividad que se inscribe en el marco de la finalidad.

El respeto al principio de finalidad supone que efectivamente el usuario tiene conocimiento de las familias de finalidades en las cuales servirá la información en el seno de las redes de los servicios públicos. La noción de finalidad tiene que estar, de ahora adelante, centrada en el usuario, no en las estructuras gubernamentales. Por ejemplo, el usuario que entra en relación con los ministerios encargados de la aplicación de las leyes sobre la seguridad de la renta de los impuestos debe saber que la información que proporcione circulará y será utilizada con la finalidad de asegurar la aplicación de las leyes relativas a la seguridad de los impuestos y que es indiferente que una tenga relación con un ministerio y la otra con un organismo público tercero. Es necesario que la información sobre las finalidades de las informaciones en posesión esté constantemente disponible y en conocimiento del usuario durante cada recopilación. Con el fin de respetar el principio de la limitación de la utilización, los espacios de información tendrán que

---

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>.

comunicar a las familias delimitadas de prestaciones, para asegurar que los datos de carácter personal serán utilizados sólo para fines relacionados y compatibles con los de la recopilación inicial.

La transparencia es una condición esencial de la credibilidad y de la confianza en los espacios en red. El usuario tiene que estar en condiciones de saber con quien tiene relación y como se concibe el proceso de información en el cual está inmerso. Por eso la evaluación pública de los espacios de información o de la compartición de información para finalidades de prestaciones electrónicas adquiere una mayor importancia. Los desafíos y los riesgos asociados a las prestaciones electrónicas que nos planteamos proponer en red se tienen que divulgar y debatir públicamente y sus riesgos se tienen que evaluar públicamente.

La calidad de los datos se aprecia en relación con las prestaciones que se tienen que cumplir: se tiene que garantizar que los datos utilizados para efectuar la prestación son exactos, precisos, están autorizados por las leyes y no presentan ningún equívoco. La legitimidad de circulaciones parecidas de datos de carácter personal están reforzadas cuando un ciudadano quiere revisar y, cuando sea procedente, rectificar en línea o por otra vía los datos que le conciernen. El derecho de rectificación, hasta ahora tan poco ejercido, consigue un sentido pleno.

Como los datos de carácter personal están disponibles en red, cada organismo tiene que asegurar que la información a la cual puede acceder, para llevar a cabo una prestación relativa a una persona, tiene la calidad adecuada, teniendo en cuenta las exigencias y el contexto de la prestación. Con el fin de asegurar la calidad, es necesario contar con el potencial de diálogo en directo entre la Administración y el usuario que encubren las tecnologías en red.

En este aspecto, el principio de la participación individual del interesado en las decisiones relativas al tratamiento de los datos de carácter personal adquiere en la red una nueva dimensión. En las redes es posible presentar la información que se tiene y validarla en tiempo real con el interesado. La garantía de calidad de los datos estará también reforzada por la validación de la información que el organismo efectúa durante una prestación específica.

Tratándose de la responsabilidad, cada organismo público susceptible de acceder a los datos personales en el seno de una red puede considerarse como el detentor jurídico. Por eso, cada organismo es responsable de la confidencialidad de los datos y el conjunto de los organismos responden solidariamente. Como hay una pluralidad de organismos, éstos tendrán que determinar cómo se repartirán la responsabilidad de los participantes. De hecho, es importante precisar las obligaciones y delimitar la responsabilidad de los gestores en relación con las exigencias de confidencialidad y de seguridad. Efectivamente, es necesario que se precisen las normas en vista de las cuales se evaluarán el comportamiento y la responsabilidad de los ciudadanos y del gestor.

La seguridad tanto física como lógica es evidentemente una exigencia esencial para cualquier entorno que funciona en red. El marco jurídico tiene que incitar a los responsables a tomar las medidas para garantizar la seguridad de los datos sobre las personas. Más allá de una cultura de la seguridad, es necesario un conjunto de procesos capaces de prevenir los ataques y, sobre todo, de solucionarlos en el momento en que se produzca un acontecimiento que ponga en peligro los procesos de tratamiento.

De esta manera, cuando los datos están en entornos de información a los que tienen acceso una pluralidad de ministerios u otros organismos o entidades públicos, la protección de los datos de carácter personal ya no resulta de las limitaciones que intervienen en el estadio de la recopilación o que prohíben la circulación. La verdadera protección proviene de un marco estricto de condiciones por las cuales es lícito acceder a los datos y de condiciones de su utilización. El marco jurídico tiene que disociar la posesión de la información y el derecho de acceder a ella y usarla.

En efecto, como los datos están en un entorno de información accesible a una pluralidad de entidades, la información está disponible, pero eso no otorga, en sí mismo, el derecho de acceso. El énfasis se desplaza hacia el derecho a utilizar los datos de carácter personal más que sobre la sola posesión o retención de los datos. Hay una disociación entre la posesión física de una información por parte de una entidad y el derecho de ésta de acceder o de usarla. A causa de su participación en un espacio en red, un ministerio u otra entidad pública tienen un conjunto de informaciones en común con otras entidades. No obstante, sólo tienen derecho a acceder a estas informaciones si es necesario para cumplir una prestación prevista por el acto constitutivo de área de compartición.

Finalmente, en el contexto de la Administración electrónica, las protecciones se tienen que concebir para garantizar que los datos de carácter personal serán efectivamente utilizados para finalidades lícitas, más que para impedir su circulación. Empiezan a emerger modelos para estructurar los modos de protección en los espacios en red. En Canadá, se habla de áreas de compartición, un concepto que se conjuga siguiendo modalidades de geometría variable según el grado de confidencialidad de los datos y se empiezan a tomar medidas de modelos fundamentados en el dominio, por parte del usuario, de las informaciones.

4.1. Las áreas de compartición de los datos de carácter personal

Ya que la circulación de datos de carácter personal entre los organismos públicos deja de tener un carácter excepcional, es mejor disponer de un marco jurídico decididamente centrado en las condiciones que se tienen que respetar durante el despliegue de prestaciones de servicios en línea. También son necesarias garantías durante el establecimiento de espacios de circulación de datos personales. Desde el punto de vista jurídico, los espacios-red en los cuales circulan datos personales tienen que estar enmarcados por reglas que precisen las responsabilidades del conjunto de las entidades concernidas. En suma, se trata de establecer reglas que designen quien responde de las informaciones repartidas en red. Para hacerlo, es importante recibir las premisas sobre las cuales reposan la mayoría de las leyes sobre la protección de datos de carácter personal que reflejan a menudo el postulado que la protección de datos está asegurada por su confinamiento.

El área de compartición es una de las nociones desarrolladas para pensar en los nuevos modelos de compartición en los entornos en red. El área de compartición se puede definir como un espacio de información en el cual los datos de carácter personal necesarios para la concesión de un conjunto de servicios llevados a cabo en beneficio de los ciudadanos pueden estar disponibles para diferentes

entidades.[24] Estos servicios o prestaciones tienen un carácter complementario y para llevarlos a cabo son necesarias informaciones que están en posesión de una pluralidad de entidades unidas por un acuerdo. La noción proporciona un concepto adaptado a las realidades de las redes y permite concebir los derechos y las obligaciones del conjunto de socios de la administración electrónica.

El concepto lleva a un conjunto de mecanismos que señalan la circulación de la información y delimitan los usos. Se trata de organizar el espacio en el seno del cual pueden circular los datos. El marco que se deriva define los derechos y las responsabilidades. Las protecciones se conciben para garantizar que los datos serán efectivamente utilizados para finalidades lícitas, más que para impedir su circulación.

4.2. Los repertorios de informaciones personales sobre la salud disponibles en línea con el consentimiento del paciente

Según diferentes condiciones, las disposiciones incluidas en las legislaciones de diferentes países organizan el alojamiento y la circulación controlada de los datos sobre la salud para finalidades asistenciales. Por ejemplo, en la legislación francesa y quebequesa, se ha instituido un régimen jurídico para los espacios de información en los cuales los datos de carácter personal necesarios para la concesión de un conjunto de servicios llevados a cabo en beneficio de los ciudadanos pueden estar disponibles para diferentes entidades. Las informaciones sólo están disponibles para los servicios o prestaciones de salud que tengan carácter complementario. Esta disponibilidad de informaciones para una pluralidad de entidades —como los médicos, otros profesionales de la salud o los hospitales— comporta unas condiciones estrictas.

En el derecho francés es la *Loi relative aux droits des malades*[25] (Ley relativa a los derechos de los enfermos) que introduce el artículo L. 1111-8 en el *Code de la santé publique* (Código de la salud pública). Esta disposición organiza el régimen jurídico del contrato de alojamiento. En términos del artículo L.1111-8, "la prestación de alojamiento es objeto de contrato". Dispone que:

> *Los profesionales de la salud o los establecimientos de salud o el interesado pueden presentar datos personales sobre la salud, recopilados o producidos en actividades de prevención, de diagnóstico o de cuidado, delante de personas físicas o morales admitidas a este efecto.*

Cuando la posesión material de los datos se transfiere a la entidad responsable del alojamiento, ésta se convierte en depositaria. Sólo las entidades responsables de alojamiento admitidas están autorizadas a cerrar un contrato de alojamiento. Para la entidad responsable del alojamiento, la falta de consentimiento expone a una sanción penal y a la nulidad del contrato. Las partes del contrato son los

---

24 En este sentido véase: 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 Ley nº. 2002-303, de 4 de marzo de 2002, D.O. 5 marzo 2002.

profesionales de la salud, los establecimientos de salud y el interesado. El acuerdo de ésta última es una condición de validez del contrato. Isabelle Vacarie afirma que:

> *Para cada paciente hospitalizado en un establecimiento de salud público o privado, el Código de la salud pública prescribe la constitución y conservación de una historia clínica. Pero el Código autoriza la externalización de las historias a una entidad responsable. A este respecto, el código precisa que "este alojamiento de datos sólo se puede dar con el consentimiento expreso del interesado". Su acuerdo es pues una condición de validez del contrato. El contrato comporta obligaciones esenciales. La entidad responsable del alojamiento asume la obligación de restitución de los datos. Como depositaria, esta entidad asume la obligación de no utilizar los datos. No puede romper el secreto.*[26]

El estatus de entidad responsable del alojamiento está regido por las disposiciones de orden público: la entidad responsable del alojamiento sólo puede recibir datos si ha sido admitida y está obligada por el secreto profesional. Así, el "depositario natural" de los historiales clínicos y la entidad responsable del alojamiento están sujetos a un mismo cuerpo de reglas de orden público. Un decreto precisa las condiciones del consentimiento y los controles ejercidos en relación con las entidades responsables del alojamiento de datos sobre la salud. El decreto señala seis condiciones a cumplir para pedir el consentimiento. Así, los contratos entre las entidades responsables del alojamiento y los clientes tienen que incluir cláusulas obligatorias y estas entidades tienen que elaborar y respetar una política de confidencialidad y seguridad.

En el Quebec, es la *Loi modifiant la Loi sur les services de santé et les services sociaux*[27] (Ley de modificación de la Ley sobre los servicios de salud y los servicios sociales) la que introduce un régimen jurídico completo para los servicios regionales de conservación de algunos datos para la prestación de servicios sanitarios. Estas disposiciones instituyen un título II intitulado "Servicios regionales de conservación de algunos datos para la prestación de servicios de salud".[28]

El artículo 520.5 de la *Loi sur les services de santé et les services sociaux* (Ley sobre los servicios de salud y los servicios sociales) pronuncia finalidades-objetivos que pretenden los servicios regionales de conservación de datos sobre la salud. Los objetivos se precisan en el artículo 520.5. Se trata de proporcionar a las partes interesadas habilitadas la información pertinente, organizada, integrada y actualizada para facilitar el conocimiento rápido de los datos sobre la salud de una persona en el momento

---

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* (Ley de modificación de la Ley de servicios de salud y servicios sociales y otras disposiciones legislativas), L.Q., 2005, c. 32, art. 189.

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, volumen 260, Cowansville, Éditions Yvon Blais, 2006.

de hacerse cargo o durante cualquier prestación de servicios de salud proporcionados por estas partes interesadas, en continuidad y en complementariedad con los proporcionados por otras partes interesadas. La otra finalidad mencionada en la Ley es asegurar la eficacia de la comunicación ulterior de los datos guardados por una agencia o un establecimiento autorizado a las partes interesadas capacitadas, con la única finalidad de prestación de servicios de salud.

La persona tiene derecho de acceso a los datos que le conciernen; puede pedir que los datos inexactos, incompletos o equívocos y los datos para los cuales la recopilación y comunicación no hayan sido autorizadas sean rectificados. La Ley también organiza los recursos con respecto a las entidades habilitadas para asegurar la conservación de los datos. También se afirma el principio de la responsabilidad y la imputabilidad de la entidad autorizada y de las otras entidades que aseguran el funcionamiento de los servicios de conservación. Por último, las entidades responsables tienen que poner en marcha un conjunto de mecanismos para asegurar la disponibilidad, la integridad, la confidencialidad, la accesibilidad y la irrevocabilidad de los datos que se poseen o se conservan. En algunos casos, es obligatorio asegurar la autenticación de la identidad de las personas habilitadas.

Sólo las partes interesadas habilitadas tienen acceso a los datos confiados a los servicios regionales y únicamente para las finalidades estrictamente delimitadas. Estos servicios de conservación sólo se pueden aplicar mediante una autorización del ministro.

Por otra parte, se aplican condiciones estrictas en relación con las medidas a tomar para asegurar la confidencialidad y la seguridad de los datos durante todo su ciclo de vida. Todo acceso a los datos se tiene que registrar y los registros se tienen que supervisar para poder detectar los accesos no autorizados. Se deben aplicar mecanismos de control interno para asegurar que las obligaciones se respetan. Está prohibido confiar a un tercero la prestación de servicios de conservación, pero es posible que un establecimiento autorizado confíe a un tercero un contrato de servicio relativo a la instalación, mantenimiento o reparación de cualquier soporte tecnológico utilizado para las finalidades de los servicios de conservación.

Cualquier persona asegurada ante la administración de seguros de enfermedad, de más de catorce años, puede dar su consentimiento para que los datos sean volcados a los centros de conservación. Previamente debe estar informada de los objetivos y finalidades perseguidos y de las modalidades de funcionamiento en relación con el acceso, la utilización, la comunicación, la conservación y la destrucción de los datos almacenados. Se le ha de especificar que el consentimiento comporta la autorización relativa a cualquier parte interesada habilitada a transmitir según su perfil de acceso de recepción. Este consentimiento es renovable. Se puede revocar en cualquier momento a petición y lo es con todo el derecho cuando una persona ya no está asegurada.

La revocación del consentimiento según los términos del artículo 520.23 comporta la desactivación de los datos conservados anteriormente. Estos datos no se pueden destruir antes de cinco años después de su inscripción. Está prohibido transmitir estos datos a una parte interesada que no proporcione a una persona servicios de salud o ejerza con respecto a una persona las funciones de control o de peritaje. También está prohibido transmitir los datos alojados a un asegurador o a un patrón y recibir extracto o

copia de los datos almacenados. Se prohíbe que cualquier persona tenga acceso a estos datos, a un extracto o una copia para la conclusión de cualquier contrato que exija la evaluación del estado de salud de una persona para un contrato de seguro o de ocupación o en cualquier otro momento. Los datos conservados no se pueden comunicar a ninguna persona, incluso con el consentimiento del interesado.

4.3. Los repertorios y los espacios virtuales bajo el control de los usuarios

El desarrollo de aplicaciones en Internet que reservan al usuario un alto nivel de control sobre las informaciones hace considerar nuevos modos de compartición de datos de carácter personal. Efectivamente, es posible poner en marcha espacios personalizados situados en parte o totalmente bajo el control del ciudadano y que se puedan utilizar en las interacciones de éste con la Administración. Unos espacios informáticos de estas características, situados bajo el control del usuario, como una red informática, le permiten situar los documentos en un espacio bajo su control. Se distinguen de la "ventana única", que son normalmente sitios que federan servicios de procedencia múltiple. La noción de espacio ciudadano nos remite más a espacios virtuales en los cuales está permitido que el usuario vuelque, conserve, autorice la consulta o la transmisión de datos con la finalidad de asegurar la realización de prestaciones electrónicas de servicios.

El modelo refleja una tendencia asociada a lo que se denomina Web 2.0, basado (SOIT) en un gran control por parte del usuario de la información almacenada y disponible a otros según su elección. El desarrollo de este tipo de contextos en línea que permiten intercambiar y compartir los documentos tecnológicos está recomendado para los que quieren asegurar la protección de los documentos en posesión del estado y para el ciudadano con la finalidad de prestaciones electrónicas de servicio. Por ejemplo, el informe sobre la administración electrónica *Vers un Québec branché pour ses citoyens* ("Hacia un Quebec conectado para los ciudadanos") resalta la idea de una "página ciudadana".[29] En este espacio accesible en línea, el ciudadano podría tener acceso a las informaciones que le conciernen, consignar los documentos relativos a las relaciones que establece con los diferentes servicios y autorizar la transmisión de documentos requeridos para la realización de prestaciones en línea.

Pero hoy por hoy queda mucho por hacer para caracterizar los diferentes tipos de espacios en línea situados bajo el control del ciudadano y que le permitan consignar documentos tecnológicos y, con su consentimiento, que estén disponibles para otras entidades, especialmente los ministerios y organismos públicos en el contexto de una prestación de servicio.

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

Conclusión

En el Estado en línea, las informaciones son esencialmente circulantes, disponibles en el momento en que tienen que estarlo con el fin de llevar a cabo una prestación de servicio. Esta circulación necesita precauciones, ya que las potencialidades de acumulación y de acoplamiento de las informaciones se pueden incrementar. Ahora bien, la adhesión de una parte de la población a algunas reglas como las que prescriben las exigencias de obtener el "consentimiento libre y explícito" para cada movimiento de información personal parece difícil de conciliar con la aplicación de un marco jurídico que refleje las características de las redes y por este motivo no existiría un marco jurídico que asegurara la protección de la vida privada en el Estado en red.

La posesión en un contexto de información accesible a una pluralidad de organismos públicos, para permitirles asegurar por sí mismo o en cooperación un conjunto de servicios a los ciudadanos, sólo es factible si existen fuertes medidas para garantizar la protección de la vida privada. La formulación de un marco jurídico de estas características supone una lectura actualizada de los principios fundamentales de la protección de los datos de carácter personal. Una protección situada al nivel de los accesos por las administraciones procura una protección muy superior a la que podemos esperar de los regímenes actuales que se derivan de las leyes relativas a la protección de datos personales.

La conexión en red de los datos administrativos apunta hacia una relectura de los principios de protección para asegurar una gestión plenamente compatible con las exigencias, riesgos y desafíos que plantean las redes y las exigencias de la protección efectiva de los derechos de las personas. Para tener en cuenta los desafíos en relación con la protección de las informaciones personales, es necesario mirar con lucidez los riesgos que se derivan del carácter confidencial de los datos y del contexto inherente a la red. Los mecanismos jurídicos tienen que procurar la protección efectiva sin obstaculizar la circulación de la información que es inherente a la puesta en marcha de los servicios en red.

Los modelos emergentes para formular los marcos de los usos compartidos de los datos de carácter personal muestran las vías que extrae la adaptación del derecho a los imperativos de la virtualización. Podemos ver el aspecto que toma la modernización de los mecanismos de protección —fundados sobre el paradigma de los dosieres en papel sustituyéndolos en un marco que asegura tanto la movilidad como la confidencialidad de la información. También se compaginan las nuevas exigencias relativas a la calidad de la información requerida para asegurar los servicios públicos.

Los marcos jurídicos que tenderán a implantarse en el Estado en red tienen que garantizar tanto la plena disponibilidad de los datos a todos los que tienen que tener acceso como la protección en relación con las otras utilizaciones. Todo eso pone de manifiesto que la implantación de modelos innovadores de compartición de datos personales constituye un desafío mayor del despliegue de los servicios en línea y de la modernización de los servicios públicos.