Université de Montréal

et

Université Panthéon-Assas Paris II

# Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau

par

**Rosario DUASO CALÉS**

Faculté de droit

Thèse présentée à la Faculté des études supérieures

en vue de l'obtention du grade de

Docteur en droit de la Faculté de droit de l'Université de Montréal

et

Docteur en droit de l'Université Panthéon -Assas Paris II

Septembre, 2011

Université de Montréal

Faculté des études supérieures

Université Panthéon-Assas Paris II

Cette thèse intitulée :

**Principe de finalité, protection des renseignements personnels et secteur public : étude sur la gouvernance des structures en réseau**

a été évalué par un jury composé des personnes suivantes :

Monsieur Karim Benyekhlef, Université de Montréal

Président-rapporteur

Monsieur Pierre Trudel, Université de Montréal

Directeur de recherche

Madame Danièle Bourcier, Université Panthéon-Assas Paris II

Directrice de recherche

Madame Esther Mitjans, Université de Barcelone

Examinatrice externe

Monsieur Jacky Legrand, Université Panthéon-Assas Paris II

Membre du jury

Monsieur Vincent Gautrais, Université de Montréal

Représentant du doyen de la Faculté des études supérieures

**Résumé :** La question de la protection des renseignements personnels présente des enjeux majeurs dans le contexte des réseaux. Les premières lois en la matière au Canada et en Europe avaient pour base une série de principes qui sont encore aujourd'hui d'actualité. Toutefois, l'arrivée d'Internet et des structures en réseau permettant l'échange d'un nombre infini d'informations entre organismes et personnes ont changé la donne et induisent de nouveaux risques informationnels. Le principe de finalité, pierre angulaire des systèmes de protection des renseignements personnels, postule le caractère adéquat, pertinent et non excessif des informations collectées par rapport à l'objet du traitement et exige qu'elles soient uniquement utilisées à des fins compatibles avec la finalité initiale.

Nous retracerons l'historique de ce principe et analyserons la manière dont la doctrine, la jurisprudence et les décisions du CPVPC comme de la CNIL ont contribué à délimiter ses contours. Nous étudierons comment ce principe se manifeste dans la structure en réseau de l'administration électronique ou du gouvernement électronique et nous relèverons les nouveautés majeures que présente l'État en réseau par rapport au modèle d'État en silo, ainsi que la nécessité d'une gouvernance adaptée à cette structure. Nous examinerons également la présence de standards juridiques et de notions à contenus variable dans le domaine de la protection des renseignements personnels et nous tenterons de montrer comment la finalité, en tant que principe ou standard, a les capacités de s'adapter aux exigences de proportionnalité, d'ajustement et de mutation continuelle qui sont aujourd'hui au cœur des défis de la gouvernance des réseaux.

Finalement, il sera question de présenter quelques pistes pour l'adoption de mécanismes d'adaptation « réseautique » pour la protection des renseignements personnels et de montrer dans quelle mesure ce droit, capable de créer un cadre de protection adéquat, est également un « droit en réseau » qui possède tous les attributs du « droit post-moderne », attributs qui vont rendre possible une adaptation propre à protéger effectivement les renseignements personnels dans les structures, toujours changeantes, où circulent aujourd'hui les informations.

**Mots clés :** protection des renseignements personnels**,** vie privée, gouvernement électronique, Internet, standard juridique, principe de finalité, réseau, gouvernance

**Abstract :** Personal data protection poses significant challenges in the context of networks. The first laws on this matter both in Canada and in Europe were based on a series of principles that remain valid today. Nevertheless, Internet and the development of network-based structures that enable infinite exchange of information between institutions and individuals are changing the priorities and, at the same time, present new risks related to data protection. The purpose principle, which is the personal data protection systems cornerstone, stresses the relevance and adequate yet not excessive nature of the collected information *vis à vis* the objective of data collection. The purpose principle also requires that the information shall not further be processed in a way incompatible with the initial purpose. We will describe the origins and evolution of this principle, as well as its present relevance and scope analysing the doctrine, jurisprudence and decisions of the Office of the Privacy Commissioner in Canada and of the *Commission nationale de l'informatique et des libertés* (CNIL) in France. We will also examine how this principle is reflected in the network structure of the digital administration and of the electronic government. We will also underline the differences between a network-based State and a « silo-based » State, each needing its structure of governance. Within the context of personal data protection, we will explore the presence of legal standards and of concepts with a changing nature. An effort will be made to highlight how purpose, be it as a principle or as a standard, has the capacity to adapt to the requirements of the core principles of the current network governance, such as proportionality, adjustment and continuous mutation. Finally, the objective is to reflect on some personal data protection network adaptation mechanisms, and to demonstrate how personal data protection can work in a network that includes all « post-modern law » elements that allow for true adaptation for effective personal data protection within the ever changing structures where data is being exchanged.

**Key words:** personal data protection, privacy, electronic government, Internet, legal standard, purpose principle, network, governance

**PRINCIPE DE FINALITÉ, PROTECTION DES RENSEIGNEMENTS PERSONNELS ET SECTEUR PUBLIC : ÉTUDE SUR LA GOUVERNANCE DES STRUCTURES EN RÉSEAU**

**PARTIE 2 : Le principe de finalité comme instrument de gouvernance des réseaux en vue de protéger les renseignements personnels**

## REMERCIEMENTS

Je souhaite tout d'abord exprimer mes profonds remerciements à mon directeur de thèse, Monsieur Pierre Trudel, professeur au Centre de recherche en droit public de l'Université de Montréal (CRDP) et à ma directrice, Madame Danièle Bourcier, directrice de recherche au Centre National de la Recherche Scientifique et membre du Centre d'Études et de Recherches en Sciences Administratives Politiques (CERSA) de l'Université Panthéon-Assas Paris II et du Centre National de la Recherche Scientifique, rattaché à l'École Doctorale de droit public, science politique et science administrative de l'Université Panthéon-Assas Paris II.
Le soutien, la liberté et la confiance qu'ils m'ont accordés au cours de ces années ont réellement contribué à l'achèvement de mes travaux de doctorat dans le cadre d'une cotutelle entre l'Université de Montréal et l'Université Panthéon-Assas Paris II.
Leur ouverture d'esprit, leur complicité et tous leurs précieux conseils m'ont aidée à ne jamais abandonner l'espoir de finir cette thèse de doctorat ces dernières années.
Leur regard critique et leurs sages commentaires au sujet de mes travaux ont guidé mes réflexions et m'ont donné les outils nécessaires pour réaliser un travail scientifique très fortement inspiré d'une vision riche et toujours actualisée des enjeux relatifs au droit à la protection de la vie privée.

Je désire également exprimer mes sincères remerciements au Professeur Karim Benyekhlef qui m'a aidée à trouver la voie pour avancer dans cette thèse et m'a sans cesse encouragée à voir concrétisés mes travaux doctoraux grâce à ses mots justes et à nos riches échanges.

Mes plus vifs remerciements vont également à toutes les institutions qui ont contribué, par leur soutien financier, à ce que je puisse me consacrer à la réalisation de mes travaux de doctorat grâce à l'attribution de bourses. Ces institutions sont la Faculté de droit de l'Université de Montréal, la Faculté des études supérieures de l'Université de Montréal, le Centre de recherche en droit public de l'Université de

Montréal (CRDP), le Centre de recherche en éthique de l'Université de Montréal (CREUM) et le Conseil international d'études canadiennes (CIEC).

Je tiens également à remercier le Commissariat à la protection de la vie privée du Canada et la Commission nationale de l'informatique et des libertés de m'avoir permis de réaliser des recherches dans leurs bureaux et centres de documentation dans le cadre de mon doctorat et ont ainsi contribué à l'écriture de certaines parties de ma thèse.

**A mi familia.**

## LISTE DES SIGLES ET ABREVIATIONS

BOE : Boletín Oficial del Estado
C.A.F. : Recueil de la Cour d'appel fédérale
CERSA : Centre d'Études et de Recherches de Sciences Administratives et Politiques
C.F. : Recueil des arrêts de la Cour Fédérale
CNIL : Commission Nationale de l'Informatique et des Libertés
CNRS : Centre Nationale de la Recherche Scientifique
CPVPC : Commissariat à la Protection de la vie privée du Canada
CRDP : Centre de Recherche en Droit Public
CRID : Centre de Recherches Informatique et Droit
C.S.A. : Canadian Standards Association
ÉFVP : Évaluation des facteurs relatifs à la vie privée
EJIL : European Journal of International Law
ENAP : École Nationale d'Administration Publique
Harv. L.Rev.: Harvard Law Review
IFAI : Instituto Federal de Acceso a la Información y Protección de Datos
IIjusticia : Instituto de Investigación para la Justicia
J.O. : Journal Officiel de la République Française
J.O.C.E. : Journal Officiel de la Communauté Européenne
L.C. : Lois du Canada
L.G.D.J. : Librairie Générale de Droit et de Jurisprudence
Loi I et L : Loi Informatique et Libertés
LPRP : Loi sur la Protection des renseignements personnels
LPRPDE : Loi sur la Protection des renseignements personnels et les Documents électroniques
L.R.C. : Lois Refondues du Canada
L.R.Q. : Lois Refondues du Québec
O.C.D.E. : Organisation de Coopération et Développement Économiques
O.J. : Ontario Judgments
P.U.F. : Presses Universitaires de France
R.C.S. : Recueil des arrêts de la Cour Suprême du Canada
R.D.P. : Revue du Droit Public
S.T.E. : Série des Traités européens
U.S.C.: United States Code
U.O.L.T.J.: University of Ottawa Law and Technology Journal
U. Mich. J.L. Reform: University of Michigan Journal of Law Reform
Yale L.J.: Yale Law Journal

## INTRODUCTION

La question de la protection de la vie privée sur Internet fait l'objet de débats depuis de nombreuses années, tant au Canada qu'en Europe. Le Canada est un pays pionnier en Amérique du Nord dans l'adoption de lois sur la protection des renseignements personnels, et l'autorité de contrôle au niveau fédéral comme provincial réalise une mission de surveillance des activités des secteurs public et privé en vue de veiller au respect du droit à la vie privée des citoyens canadiens.

Un cadre de protection des renseignements personnels existe au niveau européen et chaque pays de l'Union européenne dispose d'une loi en la matière ainsi que des mécanismes de contrôle nécessaires à l'effective protection du droit à la vie privée dans le contexte actuel.

Les enjeux que nous identifions aujourd'hui dans ce domaine sont des enjeux de type global, auxquels la plupart des pays se voient confrontés dans leur mission de veiller au respect du droit à la protection de la vie privée.

Ils doivent répondre à la question de la délimitation de certains droits fondamentaux, tels que le droit à la vie privée comme conséquence de l'adoption des mesures sécuritaires, la fin de l'anonymat dans le contexte du réseau Internet ou l'utilisation, dans les réseaux sociaux, de règles ne respectant pas les principes basiques de protection des renseignements personnels, différents aspects qui témoignent du grand éventail des problématiques qui se présentent à l'heure actuelle.

Certaines notions, comme « publiquement privé » ou « confidentiellement public »[1], représentent à merveille la confusion actuelle, qui dérive notamment d'un croissant « *publicness* »[2], qui crée un bouleversement, dans le cadre des frontières traditionnellement existantes, entre ce qui appartient au domaine privé ou au domaine public.

---

[1] Miyase CHRISTENSEN, « Facebook is watching you », *Le Monde diplomatique, Manière de voir, Internet, révolution culturelle*, 109, février-mars 2010, 52, 55.

[2] Brian STELTER, « Upending anonimity, these days the web unmasks everyone », *The New York Times*, 20 juin 2011, en ligne :
<http://www.nytimes.com/2011/06/21/us/21anonymity.html?_r=2&hp> (consulté le 2 août 2011).

Face à ces phénomènes universels, nous étudions la manière dont des réponses globales peuvent avoir un impact majeur dans la défense du droit à la protection de la vie privée dans les environnements numériques.

Nous notons également que certaines initiatives très concrètes peuvent avoir des conséquences à grande échelle. C'est le cas de l'enquête menée par le Commissariat à la protection de la vie privée du Canada[3] sur le site de réseautage social *Facebook*, qui a donné lieu à des changements importants dans la politique du droit à la protection de la vie privée du site, et cela à un niveau mondial[4].

Le Commissariat canadien est parvenu à ce que l'industrie des réseaux sociaux adopte les mesures nécessaires en vue se rendre réellement conforme à la loi canadienne en matière de protection des renseignements personnels. La particularité de cette démarche tient à ce que le CPVPC a pu exercer une véritable pression sur l'industrie des réseaux sociaux en rendant public le résultat d'une enquête qui n'a fait que confirmer le fait que certains principes essentiels de la législation canadienne relative à la protection de la vie privée dans le secteur privé n'étaient pas respectés et que les utilisateurs canadiens devaient être protégés convenablement[5].

En effet, il a déclaré que, à l'expiration du délai accordé à *Facebook*, il examinerait les mesures adoptées pour se conformer aux recommandations concrètes et envisagerait ensuite de faire appel à la Cour fédérale pour faire appliquer ses recommandations[6]. La fin de l'enquête a eu pour résultat de modifier certaines pratiques, étant donné que le site a accepté de répondre aux préoccupations du CPVPC et de se conformer à la loi canadienne.

---

[3] Ci-après : CPVPC.

[4] Lire notamment à ce sujet : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche documentaire* : *Le suivi de l'enquête sur Facebook est terminé*, 22 septembre 2010, en ligne : http://www.privcom.gc.ca/media/nr-c/2010/bg_100922_f.cfm (consulté le 20 mai 2011).

[5] Rosario DUASO CALÉS, « Redes sociales y vida privada: una ecuación posible », dans Carlos G. GREGORIO et Lina ORNELAS (dir.), *Protección de datos en las redes sociales digitales: en particular de niños y adolescentes*, México DF, IFAI et IIjusticia, 2011, 195, p. 203.

[6] Lire à ce sujet : Esther MITJANS i PERELLÓ, « Ultimátum a Facebook », *La Vanguardia*, jeudi 13 août 2009.

Nous observons depuis un certain temps que l'on exige, au Canada, des réformes de la législation sur la protection des renseignements personnels relative au secteur public, afin de pouvoir bénéficier dès aujourd'hui d'un cadre actualisé et effectif pour protéger les citoyens.

En Europe, on envisage depuis quelque temps une réforme de la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[7]. Cette volonté de réforme ne fait que témoigner du besoin provenant des changements majeurs accomplis sur le plan technologique comme dans le mode de circulation des renseignements personnels, qui exigent une mise à jour de certaines règles afin d'assurer un niveau de protection adéquat des renseignements personnels.

Toutefois, dans ce nouveau contexte où les informations circulent davantage, notamment par les structures réseautiques, les principes de protection des renseignements personnels ayant vu le jour dans les années 1970 restent d'actualité. Ce type de notion est capable d'assurer une protection évolutive, apte à répondre à des besoins en constante modification.

Il nous semble important, dans cette partie introductive, d'expliquer clairement les raisons qui ont motivé le choix de ce sujet de recherche et le contexte dans lequel nous avons réalisé nos travaux.

Cette thèse a pour objet l'étude approfondie d'un des principes de base de la protection des renseignements personnels, le principe de finalité, qui prévoit que les renseignements personnels devant être traités soient exclusivement exigés par la finalité du traitement en question[8].

Ce principe va ainsi obliger à ce que les renseignements personnels soient adéquats, pertinents et non excessifs par rapport à la finalité pour laquelle ils ont été enregistrés.

---

[7] *Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, JOCE 281 du 23 octobre 1995 (ci-après Directive 95/46/CE ).

[8] Pierre KAYSER, *La protection de la vie privée par le droit*, Paris, Éd. Economica, 1995, p. 462.

De plus, ce principe doit limiter l'utilisation des renseignements personnels uniquement aux finalités par lesquelles ils ont été enregistrés ou pour des finalités compatibles avec celles-ci. Le respect du principe de finalité impose que les renseignements personnels soient collectés pour des finalités explicites, déterminées et légitimes et qu'ils ne soient pas traités ultérieurement de manière incompatible avec ces finalités.

Nous constatons que ce principe fournit une base importante en ce qui concerne la limitation de l'utilisation des informations nominatives et impose une des règles les plus importantes des systèmes de protection des renseignements personnels.
Ce *purpose specification principle* se trouve présent dans plusieurs principes et lois relatifs à la vie privée[9] et cela, en Europe, au Canada et aux États-Unis. Ce principe est intimement lié à l'encadrement des « utilisations secondaires » des renseignements personnels ou *secondary use* et, en définitive, à la question de la réutilisation des informations à caractère personnel.

Ce principe, présent dans la majorité des lois et des textes internationaux en matière de protection des renseignements personnels, a vu le jour avec les premiers instruments adoptés en la matière dans les années 1970, soit avant l'arrivée d'Internet. Nous pouvons affirmer que le principe de finalité reste de toute actualité et qu'il devient de plus en plus pertinent en vue de limiter l'utilisation à grande échelle des informations personnelles.
Nous avons voulu analyser les conditions et modalités d'application de ce principe dans le contexte actuel, fortement caractérisé par l'existence d'un nouveau modèle de structure, celle du réseau.

Le réseau, concept par excellence de la post-modernité[10], est une notion qui a aujourd'hui un impact majeur sur le mode de circulation des informations. Par réseau, nous entendons le réseau Internet, mais aussi les réseaux de chercheurs

[9] Daniel J. SOLOVE, *Understanding Privacy*, Cambridge, Massachussets, Harvard University Press, 2008, p. 130.
[10] Jacques CHEVALLIER, *L'État post-moderne*, Paris, LGDJ, 2004, p. 41.

partageant des données scientifiques dans le cadre de leurs recherches[11], ou encore le réseau social permettant un partage massif des informations entre de très nombreuses personnes.

Ce réseau prend de multiples formes et entraîne une circulation accrue des informations, tout en conditionnant les modes d'échange des renseignements à caractère personnel.

Dans le cadre de nos recherches, nous notons que ce principe de finalité peut jouer un rôle majeur dans la gouvernance[12] des questions relatives à la protection des renseignements personnels au sein des structures en réseau.

Il nous a semblé important de nous centrer sur un réseau en particulier, afin de comprendre les enjeux qui se posent en matière de vie privée, et de pouvoir ainsi développer nos idées à l'aide d'un exemple concret.

Notre choix n'a pas été laissé au hasard et nous avons élu, dans le cadre de nos recherches, le modèle représenté par l'État en réseau, soit un gouvernement ou une administration électronique, afin de comprendre comment se dessinent les modes de gouvernance des questions relatives à la protection des renseignements personnels dans ce contexte.

Pour saisir l'importance de ce concept de gouvernance dans un scénario de gouvernement électronique, « il suffit de référer à la nécessité d'associer tous les partenaires pour assurer le développement harmonieux d'un territoire donné »[13]. Voici comment P. Trudel conçoit la gouvernance des questions relatives à la protection des renseignements personnels dans l'État en réseau :

---

[11] Anne-Marie DUGUET, « La collecte de données médicales et les échanges de données pour les recherches biomédicales et en santé publique. La législation française et ses conséquences sur l'évaluation des projets multicentriques », Jean HERVEG (dir.), *La protection des données médicales : les défis du XX^e^ siècle*, Louvain-la-Neuve, Anthémis, 61, p. 74.
La problématique dans ce contexte est celle du changement de finalité et l'utilisation secondaire des données.

[12] Pierre TRUDEL, « Hypothèses sur l'évolution des concepts du droit de la protection des données personnelles dans l'État en réseau », dans María Verónica PÉREZ-ASINARI et Pablo PALAZZI (dir.), *Défis du droit à la protection de la vie privée, Perspectives du droit européen et nord-américain*, Cahiers du CRID, nº 31, Bruxelles, Bruylant, 2008, 531, p. 534.
Pour cet auteur, la notion de gouvernance correspond à « la manière d'orienter, de guider, de coordoner les activités d'un pays, d'une région, d'un groupe social ou d'une organisation privée ou publique. Le mot est ancien mais il connaît un regain de popularité depuis une décennie ».

[13] *Id.*, p. 535.

> « Les normativités juridiques concourent avec les normativités administratives, technologiques et politiques à encadrer les interactions et les échanges d'informations au sein de l'appareil gouvernemental. La protection des données personnelles doit être pensée en tenant compte de ces phénomènes qui paraissent inhérents à l'État en réseau. Plus globalement encore, il faut constater que la société de l'information fait éclater et rend de plus en plus obsolètes les fonctionnements cloisonnés qu'ils soient le fait de l'État lui-même ou de la société civile. »[14]

Il est particulièrement intéressant pour nous d'étudier cet État en réseau puisqu'il vise dans le même temps secteur public et protection des renseignements personnels détenus par les organismes publics. C'est donc la protection des renseignements personnels détenus par les organismes publics que nous analyserons. En effet, quand les premières lois sur la protection des renseignements personnels ont été adoptées, le but était de protéger le citoyen face à la puissance de l'État, désormais capable de rassembler la totalité des renseignements concernant l'ensemble de la population.

La crainte d'un profilage massif et de l'utilisation de numéros d'identification uniques, capables de regrouper la totalité des informations concernant chacun de nous, a motivé l'adoption de législations sur la protection des renseignements personnels en vue d'encadrer les dérives pouvant potentiellement découler de l'informatisation du secteur public.
La structure qui a prévalu durant des années a été celle d'un État en silo, où les bases de données de chaque organisme étaient convenablement séparées et cloisonnées, et où l'étanchéité des fichiers était la règle générale. Les règles qui, en matière de protection des renseignements personnels, ont encadré cette structure en silo, doivent depuis quelques années faire face à une nouvelle structure étatique.

Ce nouveau modèle d'État est celui du réseau, qui a vu le jour face au modèle du silo et qui provoque un véritable changement dans le mode de circulation des informations à caractère personnel. Les lois adoptées dans les années 1970 sont

[14] *Id.*

censées encadrer de plus en plus des structures réseautiques où les fichiers détenus par chaque organisme à caractère public font l'objet d'échanges et de communications, ce qui a fait augmenter considérablement la circulation des renseignements personnels et a provoqué l'apparition de nouveaux risques informationnels.

Nous avons voulu examiner la manière dont le principe de finalité s'adapte et s'applique au modèle d'État en réseau et comment il encadre la structure réseautique de notre administration dans le but de protéger les renseignements personnels. Comment ce principe, qui a été conçu pour encadrer un État de type silo, va être capable de continuer à limiter la communication et l'utilisation des renseignements personnels dans un contexte complètement différent, caractérisé par une structure réseautique où les informations ont tendance à être réutilisées.
Y. Poullet affirmait, lors de sa participation au séminaire « État de droit et virtualité » (Montréal, octobre 2007), que l'apparition de risques nouveaux pour l'autonomie entraîne l'affirmation des principes de finalité et de transparence, tous les deux étant les principes-clés des législations de protection des données personnelles[15]. Il a également abordé la remise en cause des principes de finalité et de compatibilité des finalités, puisque, de plus en plus, dans le cadre d'Internet, la finalité est non définie et les personnes trouvent un intérêt à utiliser une donnée à des fins diverses[16].

Il sera question, dans la partie préliminaire, de retracer l'historique du principe de finalité, notamment dans le secteur public et l'administration, afin de comprendre dans quel contexte ce principe a été adopté et érigé comme un des principes de base de la protection des renseignements personnels. Dans cette partie, nous aborderons également le rôle que le principe de finalité peut jouer dans un gouvernement ou une administration électroniques, caractérisés par l'offre, pour le citoyen, de

[15] Yves POULLET, *Le cyberespace v.(?) la vie privée*, Conférence dans le cadre du Séminaire international « État de droit et virtualité », Montréal, les 23 et 24 octobre 2007, en ligne: www.etatdedroitetvirtualite.net/videos.html (consulté le 20 mai 2011).
[16] *Id.*

prestations de services électroniques[17] et par un volume croissant de partage d'informations.

Nous chercherons à connaître les dispositions faisant référence au principe de finalité dans les lois sur la protection des renseignements personnels au Canada et en Europe, et dans quelle mesure ces textes ont pour base un ensemble de principes de protection formant un cadre de protection de la vie privée assez similaire.

Nous analyserons, dans la première partie, la manière dont la doctrine, la jurisprudence et les décisions des autorités de contrôle et de protection de la vie privée en Europe et au Canada ont contribué à la délimitation des contours du principe de finalité, et étudierons des notions telles que le détournement de finalité ou l'extension de finalité dans le contexte européen ainsi que les concepts de l'usage compatible ou des fins acceptables, dans le cas canadien, afin de comprendre le degré de complexité de ce principe, complexité qui lui accorde d'ailleurs un intérêt particulier dans le domaine de la protection des renseignements personnels.

Une des grandes questions de cette première partie – et de nos travaux en général – est celle de la présence de standards juridiques et de notions à contenu variable dans le domaine de la protection des renseignements personnels. Nous envisagerons notamment le rôle que principe de finalité peut jouer dans l'actualité et cela à cause de sa nature plutôt proche de celle du standard.

En effet, nous tenterons de montrer de quelle manière la finalité, en tant que principe ou standard, a les capacités de s'adapter aux exigences de proportionnalité, d'ajustement et de mutation continuelle qui sont aujourd'hui au cœur des défis de la gouvernance des réseaux.

---

[17] Kenneth KERNAGHAN, « L'évolution vers l'état virtuel : intégration des services et des canaux de prestations des services en vue d'une prestation axée sur le citoyen », (2005), *Revue internationale des sciences administratives, L'e-gouvernance : défis et opportunités pour la démocratie, l'administration et le droit*, vol. 71-1, 129, 140.
Cet auteur évoque différentes questions mettant en évidence la nécessité de gérer les canaux de prestation des services « afin de concilier les valeurs propres au service public que sont l'efficacité, l'efficience et le service et celles qui sont la loyauté et l'équité ».

Nous aurons l'occasion également d'analyser la façon dont les standards relatifs à la finalité éclatent parfois en sous-standards, que nous retrouvons assez facilement dans le contexte des dossiers relatifs à ce principe, ce qui témoigne de l'adaptabilité et du changement perpétuel caractérisant les contextes où opèrent ces standards.

Nous procéderons également à l'observation de « données brutes » provenant d'un échantillon de dossiers portant sur des questions relatives à la notion de finalité au Canada et en Europe, en vue de démêler quels sont les « faits » gravitant autour de ces standards. Cette vision factuelle va nous servir à mieux comprendre quelles sont les démarches à suivre pour la délimitation des contours du principe de finalité dans la pratique, en vue d'analyser comment se réalise la pondération des intérêts dans le contexte de chaque dossier et comment s'applique la règle de la proportionnalité quand il est question d'apprécier si le principe de finalité est observé ou pas.

Finalement, dans la seconde partie, nous tenterons de démontrer la grande pertinence du principe de finalité en tant qu'instrument de gouvernance[18] des réseaux en vue de protéger les renseignements personnels. Le fait que la nature d'un tel principe et ses attributs peuvent être assimilés à ceux du standard juridique, fait de cette notion une des bases de la protection de la vie privée dans un contexte caractérisé par la circulation croissante des informations et où s'observe de plus en plus clairement la tendance à vouloir réutiliser les informations concernant les citoyens.

Nous analyserons la manière dont, aujourd'hui, le modèle de partage d'informations à caractère confidentiel est basé sur un système comportant notamment des règles constituant une exception au cadre général. Si nous observons les règles encadrant la communication des renseignements personnels, nous constatons qu'il s'agit d'un système basé sur la sédimentation de lois, de

[18] Stéphane ASTIER, « Une régulation éthique de l'internet : les défis d'une gouvernance mondiale », (2005), *Revue internationale des sciences administratives, L'e-gouvernance : défis et opportunités pour la démocratie, l'administration et le droit*, vol. 71-1, 143, 144.
L'auteur nous rappelle qu'« il n'existe pas aujourd'hui un mais une foule de paradigmes de gouvernance ayant une action efficace sur l'Internet ».

normes à caractère exceptionnel et sur l'accumulation des régimes destinés à contourner la règle générale.

Si le régime général impose de franches limites à un partage d'informations sans garanties pour les citoyens, nous observons des articles de loi constituant de véritables catalogues d'exceptions qui ne font qu'affaiblir le régime général.

Certains instruments, tels que les ententes bilatérales entre organismes en vue de partager des informations, nous font plutôt penser à des silos qui communiquent entre eux et contribuent à créer une situation exceptionnelle par rapport au cadre général. Ce type d'entente ressemble à un procédé « de transition » vers des outils plus adaptés au modèle réseautique.

Il sera question dans cette deuxième partie de présenter quelques pistes pour l'adoption de mécanismes d'adaptation « réseautique » pour la protection des renseignements personnels qui nous semblent plus adaptés aux nouvelles structures de circulation des renseignements personnels. Cette liste, non exhaustive, laisse entrevoir que certains outils peuvent contribuer à la mise en place d'une gouvernance des réseaux permettant la circulation des renseignements personnels, mais toujours en protégeant la vie privée des titulaires des renseignements.

Dans ce nouveau modèle de gouvernance, le principe de finalité reste éminemment pertinent et il est intéressant de constater que les nouveaux standards basés sur le critère de la finalité peuvent être d'une grande utilité dans l'encadrement de l'État en réseau. De plus, il est aujourd'hui essentiel d'établir et renforcer certains principes, comme préconisé depuis quelques années en Europe et au Canada, en vue de reformer les textes en vigueur actuellement.

Il s'agira enfin d'analyser quelles sont les transformations du droit actuel nécessaires en vue de réaliser une véritable adaptation réseautique des systèmes de protection des renseignements personnels aux conditions prévalant dans les environnements en réseau. Ce droit relatif à la protection des renseignements personnels est un « droit en réseau » créé pour encadrer le réseau, afin de donner la possibilité au droit de s'adapter à la structure sociale, confirmant ainsi les propos de

ceux qui affirment l'existence d'une homologie entre la structure sociale et la structure juridique[19].

Ce droit présente également tous les attributs du « droit post-moderne », qui sont ceux qui vont rendre possible une véritable adaptation réseautique afin de protéger affectivement les renseignements personnels dans les structures, toujours changeantes, où circulent les informations à caractère personnel.

Il nous reste à affirmer notre désir de présenter un travail de recherche pouvant apporter des éléments à inclure dans le profilage de la gouvernance de la question de la protection des renseignements personnels dans le contexte des structures en réseau. Au moment où nous assistons à la volonté de créer un cadre capable de protéger efficacement la vie privée face à des phénomènes nouveaux et toujours changeants, l'étude d'un des principes de base des systèmes de protection nous paraît essentielle et révélatrice de sa pertinence.

[19] Charles-Albert MORAND, *Le droit néo-moderne des politiques publiques*, Paris, LGDJ, 1999, p. 207.

**PARTIE PRÉLIMINAIRE : Le principe de finalité comme pierre angulaire des systèmes de protection des renseignements personnels dans le secteur public et l'État en réseau**

## CHAPITRE 1 PRINCIPE DE FINALITÉ ET L'ÉTAT COMME MODÈLE DE « RÉSEAU »

Cette partie préliminaire a pour objectif d'aborder la problématique qui se trouve à l'origine de notre recherche. Il sera question, dans un premier temps, de retracer l'historique du principe de finalité à l'égard de la protection des renseignements personnels, et de montrer à quel point ce principe est fondamental dans la détermination du mode de circulation des informations dans le secteur public. Nous tâcherons de comprendre pourquoi le législateur a accordé une telle importance à ce principe et nous nous interrogerons sur l'idée qui a amené à faire de cette notion de finalité une des pierres angulaires des systèmes de protection des renseignements personnels.

Nous aborderons le rôle complexe que joue ce principe dans le contexte de l'administration pour, plus tard, évoquer la place qu'un tel principe est voué à occuper dans la gouvernance d'un État en réseau.

Nous étudierons également les changements majeurs qui dérivent de la mise en place de ce nouveau modèle d'administration et dans quelle mesure le principe de finalité va devoir répondre aux besoins de protection des renseignements personnels, tout en respectant la mise en place des impératifs du bon fonctionnement de l'administration.

Ce sera pour nous l'occasion de présenter ces premières réflexions sur le nouveau modèle de circulation des informations et sur le cadre visant à protéger la vie privée.

Nous traiterons du rôle des principes de protection des renseignements personnels aujourd'hui, tant en Europe qu'au Canada, pour constater la grande importance et pertinence de tels principes dans le présent comme dans l'avenir.

Finalement, nous verrons dans quelle mesure le principe de finalité constitue le principe directeur des textes législatifs européens et canadiens, au travers de l'analyse de textes applicables au secteur public et privé.

## SECTION 1 Le principe de finalité comme principe fondamental pour le mode de circulation des informations dans le secteur public

L'importance du principe de finalité résulte surtout de sa fonction, qui vise à encadrer les flux de renseignements personnels. Cette fonction est d'une grande importance, notamment dans le contexte de l'administration publique, où les informations concernant les citoyens circulent davantage. Parcourir l'historique du principe de finalité va nous aider à comprendre quel est l'objectif qui a motivé l'adoption d'un tel principe et la complexité qui entoure son application.

### 1- L'objectif du principe de finalité dans le contexte de l'administration

Par le passé, nous avons cru résoudre le grand problème que posait la création d'énormes banques de données détenues par les différents organismes composant l'appareil étatique en évitant et en empêchant leur croisement. Les lois en matière de protection des renseignements personnels ont clairement eu la vocation d'être les « gardiennes » de la séparation entre les différentes bases de données du secteur public.

Il est dès lors essentiel de comprendre la pertinence de l'étude du principe de finalité pour ce qui ressortit à la protection des renseignements personnels dans le secteur public, afin de saisir pourquoi ce concept est placé au centre de nos recherches.

Le législateur a adopté le principe de finalité en vue limiter la réutilisation des informations à des fins autres que celles qui ont motivé leur collecte. Ainsi, ce principe est à la base d'un système de protection articulé autour d'un ensemble de principes créant un cadre de protection pour les renseignements personnels. Au moment où les premières lois en la matière ont vu le jour, les risques, pour ce qui est du respect du droit à la protection de la vie privée, se posaient essentiellement par rapport au secteur public.

Ainsi, suite aux craintes suscitées par les projets d'interconnexion des différentes bases de données du secteur public, il a été question d'éviter le rapprochement des renseignements personnels. La limitation de l'utilisation des informations sur les citoyens aux seules finalités ayant motivé leur traitement était à la base d'un tel dispositif.

Le cloisonnement des informations contenues dans les bases de données détenues par les différents organismes formant l'appareil étatique était l'objectif et le résultant d'une telle régulation. La règle générale que le principe de finalité visait à établir, était d'empêcher le partage d'informations entre les différents organismes et les exceptions à cette règle étaient encadrées de façon à les limiter le plus possible.

Il a existé, dans le passé, l'idée selon laquelle on devait empêcher les « investigations au second degré », pouvant découler du rapprochement de données éparses « par le moyen de l'interconnexion de fichiers distincts ou encore le traitement de données contenues dans le même fichier »[20]. C'est ici que le principe de finalité peut jouer un rôle important afin d'empêcher des pratiques de cette nature, pouvant porter préjudice au citoyen.

Bien sûr, le principe de finalité a très clairement commandé les modes de circulation des informations concernant les citoyens grâce aux limitations que les lois ont établies et que nous analyserons dans les pages qui suivent.

L'objectif visé par le législateur à l'heure de consacrer le principe de finalité, de façon plus ou moins explicite selon les différents textes des différents pays, était fondamentalement de limiter l'utilisation des données personnelles aux seuls usages ayant motivé leur traitement. Il s'agissait également d'empêcher une « réutilisation généralisée » des données personnelles à des fins étrangères à la raison pour laquelle les données avaient fait l'objet d'une collecte auprès de la personne concernée.

Au moment où les premiers textes en la matière ont vu le jour, la plus grande menace venait du secteur public puisque les administrations étaient les plus importantes détentrices de renseignements sur les citoyens.

---

[20] André ROUX, *La protection de la vie privée dans les rapports entre l'État et les particuliers*, Paris, Economica, 1983, p. 91.

L'idée qui est à la base de ce principe de finalité est celle qui a empêché une « interconnexion généralisée » de tous les fichiers existants au sein de l'administration publique. Nous aurons l'opportunité de comprendre dans les pages qui suivent la façon dont ce principe, dès l'origine, a été intimement lié à cette idée d'interconnexion, mais également à celle d'identifiant unique.

La question des interconnexions et celle de l'identifiant unique, permettant de relier la totalité des informations concernant un citoyen, sont les deux illustrations qui nous aident à comprendre quels sont les dangers qui ont inspiré le législateur à l'heure d'introduire le principe de finalité.

Comme André Vitalis l'a souligné en 1981, « à partir du moment où deux administrations stockent des informations sur les mêmes entités, une fusion de fichiers est envisageable »[21] et l'idée, dans le passé, était donc d'utiliser que, « pour remplir correctement sa fonction de clé de passage d'un fichier à l'autre (…) [une identification] doit être unique, fiable et rapide »[22].

La doctrine française a très souvent étudié la question des identifiants, toujours en soulignant l'importance du fait que l'utilisation de chaque identifiant sectoriel doit être limitée à son domaine afin d'éviter qu'il puisse se généraliser et ainsi servir en toutes circonstances à l'identification.

Ce besoin a conduit à la définition du principe de finalité « dont l'application peut s'avérer délicate »[23]. Ainsi, pour certains, l'identifiant sectoriel, « au domaine délimité par le principe de finalité, est un outil de protection de la vie privée »[24].

À partir du moment où l'idée de l'identifiant sectoriel a été privilégiée par rapport à celle d'un identifiant universel, les choses ont beaucoup changé, mais les risques ont persisté : la conception selon laquelle l'identifiant donne la possibilité d'exercer un

[21] André VITALIS, *Informatique, Pouvoir et Libertés*, Paris, Economica, 1981, p. 79.
[22] *Id.*, p. 80.
[23] Voir à ce propos : Etienne DUBUISSON, *La numérotation des personnes physiques*, thèse de doctorat, Paris, Faculté de droit, Université Paris XI, décembre 2004, p. 186.
[24] *Id.*, p. 188.

pouvoir illimité grâce à l'informatique reste d'actualité par la mise en réseau ouverte des informations sur les citoyens.

Nous observons également que le modèle d'administration « en silo », où les traitements de données personnelles appartenant au secteur public restaient séparés, s'est foncièrement fondé sur l'esprit ayant inspiré le critère de la finalité. En effet, ce principe de finalité devait empêcher le partage d'informations entre les différents organismes faisant partie de l'appareil étatique.

Comme certains l'ont souligné en 1971 déjà, « des multiples domaines d'activités du secteur public permettent d'illustrer cette conception du service public en tant qu'agent de traitement de l'information enregistrée »[25]. Pour cette raison, nous considérons que l'étude de la notion se trouvant au cœur du principe de finalité dans le contexte du secteur public, doit guider notre réflexion.

De plus, il faut se rappeler du fait que « c'est un lieu commun de remarquer que toute notre existence est jalonnée de documents de caractère personnel »[26], entre autres les certificats de naissance, les dossiers scolaires, les dossiers médicaux ou les documents relatifs à l'impôt sur le revenu.

Nous pouvons affirmer que le principe de finalité est à la base de tous les autres principes et constitue la pierre angulaire des systèmes de protection des informations à caractère personnel.

Ainsi, pour certains auteurs, le principe de finalité peut être considéré comme la « colonne vertébrale » de la Loi relative à l'informatique, aux fichiers et aux libertés de 1978[27] ainsi que de sa version modifiée après la transposition de la Directive 95/46/CE, puisque toutes les dispositions de base de celle-ci en dérivent. C'est encore relativement à ce principe que la Commission nationale de

[25] G.B.F. NIBLETT, *L'information numérique et la protection des libertés individuelles*, Paris, O.C.D.E., 1971, p. 10.
[26] *Id.*, p. 17.
[27] *Loi relative à l'informatique, aux fichiers et aux libertés* (nº 78-17 du 6 janvier 1978), J.O. 7 janvier 1978 et rectificatif du 25 janvier 1978 (Loi du 6 janvier 1978) (ci-après: Loi I et L).

l'informatique et des libertés[28] en France examine l'application des dispositions de cette même Loi[29].

Les textes canadiens et européens exigent que chaque traitement automatisé contenant des renseignements personnels ait été initialement créé pour une certaine finalité.

Le choix d'une finalité va permettre de déterminer qui aura accès à ces informations, le type de renseignements qui seront traités et oblige à ce que ces derniers soient pertinents et non excessifs par rapport à la finalité choisie initialement. De plus, ce choix va déterminer quels seront les destinataires ou les utilisateurs des renseignements, ainsi que la durée de conservation des informations, qui doit être en adéquation avec la finalité retenue.

Certains nous rappellent que c'est uniquement en connaissant l'objectif pour lequel les données ont été rassemblées, mises en mémoire et communiquées et non en raisonnant dans l'abstrait qu'il sera possible de « tracer la limite de tolérance acceptable pour l'intéressé »[30]. En effet, le principe de finalité aide la personne concernée à prévoir les différents usages dont ses données personnelles pourront faire l'objet dans le contexte du secteur public. Ce principe était destiné à établir une certaine certitude en ce qui concerne l'utilisation des informations sur les citoyens dans l'appareil étatique.

Nous considérons que, dans les dernières années, grâce à l'adoption d'une multitude de textes normatifs de natures très différentes et à l'édiction de certaines lois qui protégeaient les renseignements personnels détenus par des organisations appartenant au secteur public et au secteur privé, nous avons pu résoudre un grand nombre de questions relatives au respect du droit à la protection des renseignements personnels.

Nous tenterons de décrypter, dans le cadre de nos recherches, quels sont les enjeux de la protection des renseignements personnels concernant les citoyens détenus par

---

[28] Ci-après : CNIL.
[29] Jean FRAYSSINET, *Informatique, fichiers et libertés*, Paris, Litec, 1992, p. 73.
[30] Yves POULLET et Thierry LÉONARD, « Les libertés comme fondement de la protection des données nominatives », dans François RIGAUX, *La vie privée, une liberté parmi les autres ?*, Travaux de la Faculté de droit de Namur, t. 17, Bruxelles, Larcier, 1992, p. 244.

les différents organismes et ministères appartenant au secteur public. Il faut noter que les organismes publics détiennent un grand nombre de renseignements personnels de nature très hétérogène concernant les citoyens, phénomène qui risque de s'amplifier avec l'avènement du gouvernement électronique.

Nous procéderons dans les pages qui suivent à l'analyse de la doctrine qui, au fil des années, a contribué à la construction de ce principe afin d'identifier quel est l'objectif ou « quelle est la finalité » se trouvant face à la notion de finalité en matière de protection des données personnelles dans le secteur public.

En effet, « la notion de finalité hante les textes *Informatique et Libertés* et, en France, il est possible d'affirmer que l'autorité de contrôle a érigé cette notion en principe, qui n'apparaissait qu'en filigrane dans la loi de 1978 »[31]. Nous aurons la possibilité, dans le cadre de nos recherches, d'analyser la manière dont la CNIL a participé à la « construction » du principe de finalité au fil des années.

Pour certains auteurs, « un grand travail de *débroussaillage* dans la conception même des traitements automatisés, de leur finalité et du respect de celle-ci, a été effectué, avec les outils de la pédagogie et de la concertation, même si certains dossiers ont suscité des vifs conflits ou ont échappé au contrôle de la CNIL »[32].

### 2- Le principe de finalité et le secteur public : une question à multiples facettes

Quand nous observons les textes en la matière, nous constatons la présence de ce principe, qui apparaît de façon plus ou moins explicite. De façon générale, nous retrouvons l'obligation de respecter ce principe, mais sans qu'il soit défini de façon concrète, ce qui complique la détermination de ses contours.

---

[31] Isabelle DE LAMBERTERIE et Henri-Jacques LUCAS (dir.), *Informatique, libertés et recherche médicale*, Paris, CNRS Éditions, 2001, p. 79.

[32] Nathalie MALLET-POUJOL, « La réforme de la Loi Informatique et libertés », *Revue française d'administration publique*, nº 89, *La protection des données personnelles*, janvier-mars 1999, 46, 59.

En effet, comme certains nous le rappellent, « les textes sont silencieux quant à la définition du terme “finalité”, mais cela ne les empêche pas d’utiliser cette notion »[33]. Cependant, malgré l’absence d’une définition provenant des sources, certains ont tenté une approche sémantique de cette notion :

> « La finalité constitue la raison d’être d’un traitement particulier de données personnelles. Elle est l’objectif désigné lors de la constitution d’un traitement, dont elle commande la création. À ce titre, elle justifie les caractéristiques maîtresses du traitement (qualité des données, durée…) Elle est devenue par conséquent un des principaux paramètres qu’utilise l’autorité de contrôle pour estimer la légitimité et la légalité des projets de traitement qui lui sont soumis. »[34]

En effet, la « finalité » devient un des principaux paramètres pour déterminer si un traitement respecte les règles essentielles de protection des données personnelles. La CNIL a souligné que les fins poursuivies par un traitement ne doivent pas être formulées « d’une manière trop large ou en des termes pouvant prêter à la confusion ».[35]

La raison en est que le « principe central » de la finalité est celui qui permet à la Cnil de se prononcer sur la viabilité de l’ensemble du projet qui lui est soumis[36]. Il faut noter que la finalité s’apprécie par rapport au traitement et non par rapport à l’information, qui n’a pas de finalité prédéterminée[37].

Nous pouvons constater alors à quel point il est essentiel de cerner la finalité de chaque traitement de renseignements personnels de façon concrète et précise.

Certains ont attribué à la finalité, d’une part, une « fonction en tant que point de référence », puisque, c’est en regard de la finalité des traitements que sont appréciés la pertinence des informations traitées, la qualité de leurs destinataires, ainsi que leur durée de conservation.

---

[33] I. DE LAMBERTERIE et H.-J. LUCAS (dir.), préc., note 31, p. 79.
[34] *Id., p.* 79.
[35] J. FRAYSSINET, préc., note 29, p. 173.
[36] Voir à ce sujet : I. DE LAMBERTERIE et H.-J. LUCAS (dir.), préc., note 31, p. 79.
[37] Bruno MORIN (dir.), *Les fichiers de personnes et le droit*, Paris, Éditions Hermès, 1991, p. 56.

D'autre part, nous constatons également l'existence de la finalité « en tant que vecteur de dangerosité », puisque c'est essentiellement de l'objectif poursuivi par le traitement et du respect de la finalité que dépend la dangerosité des traitements pour la vie privée[38].

La doctrine a également attribué à la notion de finalité une fonction permettant d'établir une distinction entre les termes « donnée » et « information ».

Ainsi, l'information, pour certains, englobe la signification attachée aux données par une personne, et cela dans des circonstances déterminées. Pour exprimer cette différence, on peut dire que « le mieux est peut-être de caractériser l'information comme un vecteur plutôt que comme un scalaire, ou de dire que l'information est assortie d'une finalité »[39].

La doctrine a identifié deux critères dans le contexte du respect du principe de la spécification de la finalité, notamment pour ce qui est des conditions de légitimité expressément retenues dans les différentes législations[40].

D'une part, on parle d'un « critère de concordance », puisque certaines législations indiquent que la finalité du traitement informatique va devoir être conforme aux missions du maître du fichier et à la nature du fichier.

D'autre part, nous identifions un « critère du bien fondé du traitement », qui intéresse tout particulièrement les activités de recherche.

La plupart des textes de loi se limitent à dire que ce principe doit être respecté, sans essayer de déterminer sa nature, son étendue, ses caractéristiques et sans spécifier comment il interagit avec d'autres principes.

C'est surtout la doctrine qui émane des autorités de contrôle qui fournit les pistes incontournables pour approfondir l'analyse du principe de finalité et comprendre comment il est utilisé dans la pratique.

Il convient de noter que la CNIL, en 1996, citait dans une de ses publications les « principes d'application délicate », faisant notamment explicitement référence au

---

[38] Voir sur ces deux fonctions attribuées à la finalité : Patricia BLANC-GONNET, *Protection de la vie privée et transparence à l'épreuve de l'informatique*, thèse de doctorat, Paris, Faculté de Droit de Saint Maur, Université Paris Val de Marne (Paris XII), 2001, p. 68 et 69.

[39] G.B.F. NIBLETT, préc, note 25, p. 10.

[40] Voir notamment l'étude réalisée sur ces questions : Isabelle VACARIE, *Le traitement informatique des données de santé*, thèse de doctorat, Paris, Université de Paris I, Panthéon-Sorbonne, 1988, p. 145.

principe de finalité[41], ce qui témoigne d'une certaine complexité du principe et d'une application pour le moins difficile.

Toutefois, la CNIL signale qu'à aucun moment elle n'a affirmé que ces principes étaient inadaptés et qu'il serait plus opportun de les écarter. Ce que la CNIL prévoit, c'est qu'ils « risquent souvent de donner lieu à des dérives et que leur respect scrupuleux ne sera pas aisé à contrôler »[42].

Cette affirmation nous semble pertinente, singulièrement dans le contexte des traitements détenus par le secteur public puisque, dans le passé, nous avons observé des situations où une utilisation abusive des données personnelles concernant les citoyens a pu se produire à cause d'un détournement de finalité.

C. Marliac-Négrier a procédé à l'étude des questions entourant la protection des données nominatives informatiques en matière de recherche médicale et elle affirme que, dans ce domaine, la finalité est une « notion insuffisante » et qu'elle ne suffit pas à elle seule, « même si elle réussit à cantonner de nombreuses difficultés »[43].

Ainsi, il est signalé que le critère de finalité est souvent opposé à celui de la sensibilité des données, sauf que, jusqu'aujourd'hui, nous pouvons affirmer que la sensibilité des données dépend plus des « circonstances de lieu, de temps et d'espace que de leurs caractères intrinsèques »[44].

À cause du caractère insuffisant de la notion de finalité, cette juriste préconise la conciliation du critère de finalité avec celui qui lui est opposé, c'est-à-dire le critère de sensibilité.

Pour elle, le critère de finalité « n'est pas fiable car inconstant »[45]. Voici l'idée se trouvant à la base de cette affirmation :

> « S'il faut se référer à l'appréciation de l'extension possible opérée sous le contrôle de la CNIL, alors la personne concernée par le

[41] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Voix, Image et Protection des Données Personnelles*, Paris, La Documentation Française, 1996, p. 63 et s.
[42] *Id.*, p. 63.
[43] Claire MARLIAC-NÉGRIER, *La protection des données nominatives informatiques en matière de recherche médicale*, Tome II, Presses Universitaires d'Aix-Marseille, 2001, p. 463.
[44] *Id.*, p. 453.
[45] *Id.*, p. 462.

> traitement de données nominatives ne saura pas, au moment de la collecte, si la raison, la finalité pour laquelle elle accepte de donner les renseignements en question, sera la seule utilisée ou s'il y aura extension de finalité. De plus, il est par avance impossible de signaler quelle sera l'éventuelle nouvelle finalité attribuée au traitement, même si la connexité permet de situer le cadre. »[46]

Par conséquent, la « connexité », en tant que critère, fournit une certaine « sécurité juridique », sauf que, bien qu'il soit obligatoire de signaler la finalité du traitement envisagé directement à la CNIL et, indirectement, à la personne concernée, « rien n'est organisé pour gérer ces extensions de finalité »[47].

Dans le cadre des énormes banques de données détenues par les organismes du secteur public, nous observons également comment, par le passé, les données personnelles ont eu une certaine vocation à être réutilisées. Toutefois, le critère de connexité n'est pas toujours celui qui a justifié certains rapprochements de données ni la détermination de certaines finalités « secondaires » des informations.

Pour la CNIL, la finalité est « une notion fonctionnelle très utile »[48], puisque « c'est au vu de la finalité du traitement qu'elle apprécie la cohérence des données, la qualité des destinataires et la durée de conservation des informations ».[49]

Notons que la CNIL a jugé que la réflexion sur la finalité du traitement reste essentielle afin d'en mesurer le caractère proportionné et raisonnable. Elle déclare : « plus qu'à l'énoncé des finalités, c'est à la justification de la finalité, à la preuve de la nécessité et de l'efficacité du traitement que l'on s'attache »[50].

Nous pouvons donc affirmer que ce principe possède une nature assez subjective et indéterminée, ainsi qu'un caractère purement contextuel. Certains objecteront « l'imprécision » du principe en soulignant que la notion de finalité est « singulièrement floue » et présente le risque d'une « interprétation fort large »[51].

Pour certains auteurs, cette critique du principe de finalité reste toutefois peu fondée :

---

[46] *Id.*, p. 463 (nous soulignons).
[47] *Id*.
[48] I. DE LAMBERTERIE et H.-J. LUCAS (dir.), préc., note 31, p. 79.
[49] *Id.*
[50] Nathalie MALLET-POUJOL (dir.), *Traçage électronique et libertés*, Problèmes politiques et sociales nº 925, Paris, La Documentation Française, 2006, p. 7.
[51] Voir : Y. POULLET et T. LÉONARD, préc., note 30, p. 244.

> « Le respect du critère de la “finalité” est en effet plus souple et plus respectueux d’une appréciation judiciaire évolutive que le critère *a priori*, réglementaire, tiré de la nature soi-disant “en soi” des données, critère qui, par opposition, est peu soucieux de la réalité contractuelle. »[52]

Certains font remarquer que ce principe de finalité peut paraître, au premier abord, un peu abstrait, mais qu’« il ne l’est pas et il constitue la garantie cardinale de nos législations »[53]. En conséquence, certaines caractéristiques de ce principe qui, à première vue, peuvent paraître problématiques, deviennent celles qui permettent son application au cas par cas et qui lui accordent un rôle majeur dans les systèmes de protection des renseignements personnels.

Même si les différents instruments normatifs nous présentent la finalité comme une notion qui doit être interprétée comme « unitaire », il convient de se rappeler que le caractère complexe de ce principe tire son origine du fait que, dans certains cas, il n’existe pas une mais plusieurs finalités qui peuvent être attribuées à un traitement, sans que cela se traduise toujours par le non-respect des législations relatives à la protection des renseignements personnels.

Il s’agit alors de déterminer quelles sont les finalités « conciliables » et quelles sont les « familles de finalités » qui sont compatibles et celles qui ne le sont pas. Arriver à donner réponse à ces questions n’est pas une tâche facile. Certains auteurs se demandent : « Que faut-il entendre par traitement compatible avec la finalité initiale du traitement? Et quelles sont les sanctions de l’incompatibilité ? »[54].

Si nous parvenons à déterminer une série de finalités compatibles, nous serons en mesure d’identifier un ensemble d’usages licites des renseignements en question.

La notion du détournement de finalité mérite que l’on s’y attarde, parce que c’est en détournant la finalité des traitements contenant des renseignements personnels que

---

[52] *Id.*, p. 244.

[53] P. LECLERQ, « La CNIL, garante de la finalité, de la loyauté et de la sécurité des données personnelles », dans *Les libertés individuelles à l’épreuve des NTIC*, Marie-Christine PIATTI (dir.), Lyon, Presses Universitaires de Lyon, 2001, 111, p. 113.

[54] P. BLANC-GONNET, préc., note 38, p. 71.

l'on va pouvoir identifier un danger réel quant à la protection de la vie privée des personnes concernées :

> « Le détournement de finalité n'est pas celui de l'information à proprement parler, contrairement à ce qui est parfois écrit […] ; il faudrait dans ce sens plutôt envisager le vol du bien informationnel. En effet, les données nominatives n'ont pas des finalités en elles-mêmes, mais seulement une utilité par rapport à la finalité du traitement ; en conséquence, la finalité du traitement qui doit être seule considérée, déteint sur les informations. »[55]

Comme certains auteurs l'ont répété, c'est par rapport au secteur public que la question du détournement de finalité présente les plus grandes difficultés : « La question du détournement de finalité du traitement de données relatives à la vie privée se pose avec une acuité particulière dans le cas des applications mises en œuvre par les autorités investies de missions de service public »[56].

Certains parlent de « détournements de finalité incontrôlables », à cause de l'existence d'une pluralité de gestionnaires, ce qui peut entraîner des risques potentiels de divulgation et d'exploitation non autorisée des données. Ce qui peut nous faire penser à une « maîtrise illusoire des données » :

> « À travers le respect des principes de finalité, de transparence, de loyauté de la collecte et de l'usage, de sécurité, le principe de libre communication des informations sur soi étend son influence sur le régime des licences non volontaires. Mais la constatation perd de son évidence ; au fur et à mesure de la pérégrination des données, les règles et principes transmis en même temps qu'elles, tendent à se diluer, perdre de leur efficacité, de leur réalité. Plus l'information s'éloigne de la personne et plus l'effectivité de la maîtrise est illusoire. »[57]

---

[55] J. FRAYSSINET, préc, note 29, p. 136.
[56] Guy BRAIBANT, *Données personnelles et société de l'information, Rapport au Premier Ministre sur la transposition en droit français de la directive no 95/46*, Paris, La Documentation Française, 1998, p. 9.
[57] Frédéric LESAULNIER, *L'information nominative*, thèse de doctorat, Faculté de droit, Paris, Économie-Sciences sociales, Université Panthéon-Assas, 2005, p. 220.

Ils affirment qu'« en permettant l'interrogation croisée des données qu'elles contiennent, les banques de données informatisées présentent un risque de détournement de la finalité pour laquelle ces données ont été recueillies »[58]. Il devient alors essentiel de se demander pourquoi le traitement de renseignements personnels a été créé.

À quoi devaient servir ces renseignements personnels ? Cette question est particulièrement cruciale pour ce qui relève du secteur public et prouve la complexité qui se cache derrière l'application du principe de finalité.

La réponse à cette question est assez facile à trouver dans certains cas mais, dans d'autres, il devient compliqué de déterminer une finalité précise, à cause de la nature même des renseignements personnels.

Certains auteurs nous rappellent que toute modification ou adjonction de finalité doit faire l'objet d'une nouvelle demande et que « derrière le changement de finalité se dissimule un traitement différent pour lequel les conditions de mise en œuvre du premier traitement ne sont plus adaptées »[59].

Dans ses études, Louise Cadoux utilise l'expression « dérive de finalités » quand elle fait référence aux risques qui découlent de la vidéosurveillance dans les lieux publics : « le principe de proportionnalité ne peut évidemment se satisfaire que d'une finalité précise sans quoi il serait ruiné ; mais, en même temps, on sait que l'on recueille bien plus d'informations que celles utiles pour cette finalité ; et que là est la tentation, celle qui conduit à la dérive des finalités »[60].

Le danger d'une telle dérive existe dans tous les domaines de la protection des données personnelles mais, au sein du secteur public et dans le cadre du développement des échanges dans les réseaux gouvernementaux, le risque nous semble plus accru.

Ainsi, nous pouvons identifier, d'une part, les renseignements personnels qui peuvent être contenus dans l'ensemble des sources de nature publique détenues par

---

[58] Claude BOURGEOS, *L'anonymat et les nouvelles technologies de l'information*, thèse de doctorat, Paris, U.F.R. de droit, Université Paris V, 2003, p. 178.

[59] I. DE LAMBERTERIE et H.-J. LUCAS (dir.), préc., note 31, p. 79.

[60] Louise CADOUX, « La vidéosurveillance des lieux publics », dans *Nouvelles technologies de l'information et libertés individuelles*, Nathalie MALLET-POUJOL (dir.), Paris, La Documentation française, 1998, p. 17.

l'appareil étatique, renseignements que nous qualifions de « données publiques »[61] ; et, d'autre part, l'ensemble des renseignements personnels qui sont issus des traitements détenus par les différents organismes publics et qui, en général, ont un caractère confidentiel et ne font donc pas l'objet de publication ou de diffusion.

Nous pouvons ainsi identifier les « fichiers administratifs » élaborés à des fins administratives et qui sont « souvent des dossiers individuels organisés afin de renseigner au sujet de personnes particulières ceux qui doivent se prononcer sur leurs qualifications, leur moralité, leurs droits, les possibilités et avantages à leur offrir et les prestations à leur verser »[62].

Pour certains experts, la caractéristique de ces fichiers est « qu'éventuellement les données peuvent être consultées par des entités diverses, et en tout cas différentes de celles qui les ont constituées »[63].

Nous pouvons observer également un phénomène de « mise en réseau » des renseignements personnels concernant les citoyens, provoqué par le partage de plus en plus fréquent des informations entre les différents organismes appartenant aux multiples niveaux de l'administration publique.

Auparavant, la crainte provenait de la possibilité de regrouper, par interconnexions, des informations devant être compartimentées : « les possibilités d'interconnexion offertes par l'informatique peuvent également être utilisées pour passer d'une comptabilité sectorielle sur l'individu à une comptabilité globale »[64].

Certains affirmaient dans le passé que, « malgré le principe de finalité du fichier mais aussi d'autodétermination de l'individu fiché, il est à craindre que l'informatisation renforce le contrôle sécuritaire au détriment d'un contrôle social qui lui, utiliserait les statistiques et les modèles pour une meilleure gestion prévisionnelle de la collectivité »[65].

---

[61] Voir sur les différentes classifications de l'ensemble des données publiques et sur les enjeux liés à sa diffusion sur Internet : Herbert MAISL, *Le droit des données publiques*, Paris, L.D.G.J., 1996.
Jean-Michel BRUGUIÈRE, *Les données publiques et le droit*, Paris, Litec, 2002.
Dieudonné MANDELKERN et Bertrand DU MARAIS, *Diffusion des données publiques et révolution numérique*, Paris, La Documentation française, 1999.

[62] Guido GÉRIN, *Les effets de l'informatique sur le droit à la vie privée*, CEDAM, 1990, p. 90.

[63] I. DE LAMBERTERIE et H.-J. LUCAS (dir.), préc., note 31, p. 80.

[64] A.VITALIS, préc., note 21, p. 111.

[65] G. GÉRIN, préc., note 62, p. 104.

Mais il convient également rappeler que, d'une part, les services publics recourent souvent à des entreprises privées pour la gestion et la maintenance de leurs fichiers automatisés et que, d'autre part, il existe de nombreux services mixtes public-privé.
Mais, comme certains l'ont signalé, une distinction fondamentale « parce qu'elle touche au noyau du droit de la personnalité, a pour objet le caractère forcé ou volontaire de la collecte des informations »[66]. Voici, en quelques mots, la vision de la situation particulière qu'occupe le citoyen face à l'État :

> « Pour satisfaire à ses besoins ou obtenir certaines prestations, l'individu ne saurait manquer de contracter et d'accepter les conditions qui lui sont faites ; de plus, il occupe une situation juridique dépendante caractérisée, dans l'hypothèse de l'activité professionnelle, par le pouvoir hiérarchique de l'administration ou par l'autorité du chef d'entreprise. Le *pouvoir informatique* symbolise et renforce une telle situation : le flux informatique se nourrit des données propres à la personne qui est dans une situation dépendante et il est maîtrisé par ceux qui occupent la fonction d'autorité ou détiennent le pouvoir économique. »[67]

Par conséquent, il nous semble spécifiquement pertinent d'analyser la façon dont le principe de finalité peut arriver à compenser cette position de faiblesse du citoyen, faiblesse renforcée encore par les progrès de l'informatique.
Nous pouvons affirmer que, pour ce qui est du secteur public, « même la distinction entre la divulgation obligatoire de certaines données et celle qui est subordonnée au consentement préalable de la personne intéressée ne laisse pas d'être singulièrement artificielle »[68].
En effet, le citoyen doit fournir un grand nombre de données aux pouvoirs publics, en échange de l'obtention de certaines prestations, raison qui motive l'idée que « la liberté de consentir, qui n'est que le revers de celle de ne pas consentir, peut se trouver dans les faits réduite au point de n'être plus que purement théorique »[69].
Par le passé, avant la réforme de la Loi I et L, la finalité du traitement « pouvait être mieux cernée ou assurée et les destinataires de ces données clairement identifiés,

[66] *Id*., p. 113.
[67] *Id*., p. 117.
[68] *Id*., p. 117 et 118.
[69] Agathe LEPAGE, « Consentement et protection des données à caractère personnel », dans Jean-Luc GIROT (dir.), *Le harcèlement numérique*, Paris, Dalloz, 2005, 227, p. 248.

sans oublier les discussions sur la mise en place de procédures de sécurité auquel le maître du fichier n'aurait pas pensé »[70]. Effectivement, avec la modification de la Loi I et L, certains aspects de l'encadrement des traitements ont été changés. Nathalie Mallet-Poujol fait remarquer que le principe de finalité, même après la réforme de la loi française, demeure au centre du dispositif :

> « Espérons que cet espace "d'intelligence" de la problématique informatique et libertés (qui ne s'appliquait certes qu'aux traitements du secteur public) ne s'atrophiera pas à la faveur de la diminution des contrôles *a priori*. Toujours est-il que le principe de finalité restera la clé de voûte de la protection des données personnelles, voie essentielle de concertation pour arbitrer les intérêts en cause »[71].

Dans le cas du Québec, la Commission d'accès à l'information nous rappelle que l'étanchéité des fichiers fait office de mesure de protection des renseignements publics du secteur public :

> « Sans étanchéité de leurs fichiers de renseignements personnels, les organismes publics ne seront plus en mesure de garantir aux citoyens qu'ils respectent leur droit de savoir à quelles fins sont utilisés les renseignements personnels. »[72]

La Commission d'accès à l'information du Québec a demandé et établi sous forme de Recommandation que le concept de l'étanchéité des fichiers détenus par un organisme public soit clairement reconnu dans la Loi sur l'accès.[73]

Actuellement, il nous semble important de nous demander si le principe d'étanchéité des fichiers détenus par les organismes publics s'adapte à la nouvelle administration qui prend la forme d'un réseau et si, dans ce contexte, ce principe est le seul qui puisse servir à respecter les finalités des traitements.

---

[70] N. MALLET-POUJOL, préc., note 32, 59.
[71] *Id*. (nous soulignons).
[72] COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Une réforme de l'accès à l'information : le choix de la transparence, Rapport sur la mise en œuvre de la Loi sur l'accès et de la Loi sur le secteur privé*, Novembre 2002, p. 101.
[73] *Id.* Voir à ce sujet la Recommandation n° 40.

Certains auteurs ont souligné les difficultés qui entourent la détermination et la délimitation du principe de finalité, quand cette détermination finit par entraver l'action des différents organismes publics :

> « Ce critère (la finalité), en pratique, se heurte à des obstacles qui peuvent être insurmontables. En effet, la finalité de la constitution d'un fichier ne peut pas toujours être donnée avec précision. Cette finalité peut changer avec le temps et cela pour des motifs très légitimes. Ne risque-t-on pas d'apporter des entraves à l'action d'un organisme et de porter préjudice à son efficacité sociale? Enfin, et surtout, le critère va à l'encontre même de la logique d'une banque de données pour qui le stockage des informations prime sur leurs utilisations. Elle est naturellement portée, devant la méconnaissance des usages futurs, à stocker le maximum de données »[74].

Cependant, comme nous l'avons vu précédemment, il faut s'interroger sur la manière d'établir quelles seront les finalités compatibles pour lesquelles les renseignements sur un citoyen peuvent servir, sans que cela ne se traduise par une atteinte d'un des droits les plus fondamentaux. Et, tout d'abord, réfléchir aux changements de finalité que nous pouvons considérer comme légitimes. Toutes ces questions illustrent la complexité du principe de finalité et son application délicate dans le contexte du secteur public.

### 3- Principe de finalité et cloisonnement de l'information : historique

Nous analyserons dans les pages qui suivent l'historique de ce principe de finalité, et cela grâce à l'examen de certains textes qui sont à l'origine d'une telle notion. Cette démarche vise à comprendre dans quel contexte ce principe a été adopté pour la première fois et quel était l'objectif de ceux qui ont décidé de le placer au centre des systèmes de protection des renseignements personnels.

[74] A.VITALIS, préc., note 21, p. 154 (nous soulignons).

### A- Le premier rapport

Dès 1975, le premier Rapport de la Commission « Informatique et Libertés » ou « Rapport Tricot », ayant Bernard Tricot comme rapporteur général, a prévu la manière dont l'informatique allait permettre d'échanger des informations entre les administrations :

> « L'informatique accroît la possibilité, entre les services, d'échanges d'informations qui peuvent, selon la façon dont on les considère, apparaître comme des progrès dans le sens de l'efficacité ou comme des menaces pour les administrés. »[75]

Nous retrouvons également dans ce rapport, la crainte des « interconnexions abusives »[76] rendues possibles par le croisement des banques des données. Ce rapport identifie, en 1975, les « risques pour l'avenir », notamment basés sur la capacité de l'État « de suivre, analyser, confronter les diverses activités de la personne, de la famille (…) l'informatique agit dans le sens de l'efficacité technique, mais non dans celui de la liberté. »[77]

Nous pouvons constater que, dès 1975, d'aucuns affirment qu'il est temps de désenclaver les différents services de l'administration par la diffusion et l'échange des informations, mais que, dans le même temps, les experts se posent des questions et identifient les menaces majeures qui pourraient provenir d'un alourdissement du contrôle social et de l'aggravation des rapports inégalitaires au sein de la société : « Le jour où, au sein de l'État, chaque fonctionnaire qui détient une parcelle de la puissance publique pourrait tout savoir de chaque homme, de chaque famille, de chaque entreprise, ne voit-on pas à quels risques l'administré serait exposé? »[78].

Les rédacteurs du rapport se sont rendu compte que les dangers étaient plus visibles dans le secteur public, et affirment que « la conjonction des prérogatives de

---

[75] COMMISSION INFORMATIQUE ET LIBERTÉS, *Rapport de la Commission Informatique et Libertés*, Paris, La Documentation Française, 1975, p. 12 (ci-après : Rapport Tricot).
[76] *Id.*, p. 13.
[77] *Id.*, p. 15.
[78] *Id., p.* 17.

puissance publique et des moyens informatisés pose des problèmes, qui sous d'importantes réserves, ne se rencontrent pas au même degré dans le secteur privé »[79].
Cependant, le Rapport Tricot va plus loin et cible les problèmes posés par certains développements de l'informatique. Ce rapport a même été capable de citer, parmi tous les développements, d'une part, les interconnexions, et d'autre part, les banques des données, comme deux sources de risques pour la liberté.

Dans le cadre de nos travaux, nous allons plutôt nous intéresser aux éléments que ce Rapport, un des premiers travaux concernant la protection des renseignements personnels en France et en Europe, avance autour du concept d'interconnexion, concept relié à l'objet de notre étude de façon très claire.

Le Rapport Tricot émet une idée qui, même aujourd'hui, nous semble tout à fait d'actualité : « appliqué au domaine de l'informatique, le terme d'interconnexion provoque, dans l'opinion, méfiance et inquiétude »[80].

Nous ne pouvons pas oublier, dans ce contexte, que la parution en 1974 de l'article « "Safari" ou la chasse aux Français »[81] dans le journal *Le Monde*, dans son édition du 21 mars, a dévoilé à la société française les dangers et les risques de la mise en place de certains traitements informatiques contenant des informations concernant les citoyens.
Philippe Boucher écrit dans cet article que « le Conseil d'État en 1970, puis le Ministère de la Justice en 1972 (…) ont insisté sur la nécessité d'une intervention législative qui préciserait les quelques éléments essentiels de l'emploi de l'informatique appliquée aux particuliers : réglementation de l'accès des tiers aux fichiers, de l'intercommunication de ceux-ci, droit de rectification des personnes fichées si les renseignements sont inexacts, etc. »[82].

[79] *Id*., p. 28.
[80] *Id.*, p. 55.
[81] Philippe BOUCHER, « Safari ou la chasse aux français », *Le Monde*, 21 mars 1974.
[82] *Id.*

Les questions concernant l'interconnexion des différents fichiers de l'État semblent déjà au centre des préoccupations de tous les pouvoirs publics en France.

Sans aucun doute, l'article paru dans *Le Monde* a aidé à propager cette idée de l'interconnexion. Certains auteurs citent d'ailleurs, en 1977, les effets notoires de la campagne de presse du printemps 1974 autour du projet « Safari »[83]. Missika et Faivret nous rappellent une idée qui est au cœur du débat provoqué en France à la suite de la publication de l'article : « La logique de l'interconnexion veut que ce ne soit pas une information qui soit dangereuse mais la relation entre deux informations. »[84], une réflexion qui résulte clairement de cette campagne de presse comme de la prise de connaissance par le grand public d'une nouvelle réalité créée par les possibilités de l'informatique en ce qui concerne l'interconnexion des fichiers.

Ces auteurs se demandent également : « Comment définir la liste des informations sensibles, alors que deux données, en elles-mêmes anodines, prennent une signification dès lors qu'elles sont rapprochées ? »[85].

Derrière cette pensée, il faut lire le constat suivant : les données ne sont jamais « neutres » et c'est par le rapprochement d'informations apparemment neutres, et donc la création de profils plus précis des personnes, que la protection de la vie privée se trouve menacée. C'est aussi à partir de cette idée que le principe de finalité a été identifié comme étant celui qui permet d'empêcher les rapprochements pouvant donner comme résultat le non-respect du droit à la protection des renseignements personnels.

Il faut noter que « la finalité du traitement sert de critère de discernement et non la sensibilité des informations »[86], ce qui montre l'importance du principe comme critère dans les conditions d'encadrement de chaque traitement.

---

[83] Voir : Jean-Louis MISSIKA et Jean-Philippe FAIVRET, « Informatique et Libertés », *Les temps modernes*, Septembre-Octobre 1977, p. 421 et s.
[84] *Id., p.* 318.
[85] *Id.*
[86] I. VACARIE, préc., note 40, p. 50.

Nous notons également que, plus tard, lors des travaux préparatoires de la Loi I et L, le projet S.A.F.A.R.I. est toujours au centre des débats :

> « À cette époque, en 1975, nous étions sous le coup de l'émotion qui avait été provoqué par S.A.F.A.R.I. – système automatisé pour les fichiers administratifs et le répertoire des individus – dont on disait qu'il emmagasinait des renseignements et des fiches sur les 50 millions de personnes vivant en France en 1971. »[87]

Le Rapport Tricot[88] fait très clairement le lien entre la figure de l'interconnexion et celle de l'identifiant unique en nous rappelant cette idée : « L'interconnexion peut avoir une autre ambition : celle de rapprocher différents systèmes de traitement afin de permettre des interrogations, des réponses, des échanges qui enrichiront chaque système grâce aux apports des autres » [89].

Cependant, cette notion d'interconnexion est toujours reliée à l'idée de l'identifiant unique : « Le problème des interconnexions est lié, (…) pour ce qui est de la technique à l'identifiant unique »[90]. Bien sûr, cette mise en rapport des deux figures trouve son origine dans le projet S.A.F.A.R.I. et la très célèbre menace de « chasse aux Français ». Ainsi, cette idée a été à l'origine des craintes suivantes : « Si les interconnexions des fichiers peuvent être abusives, ce qui est vrai dans certains cas, l'identifiant commun à l'ensemble de ces fichiers comporterait un danger puisqu'il faciliterait les interconnexions »[91].

Le rapprochement entre fichiers employant des identifiants différents a donc suscité questionnements et soucis majeurs à l'heure de déterminer si ce cas était juste une possibilité théorique et plutôt aléatoire.

Finalement, on a constaté que les fichiers administratifs présentaient des éléments communs qui allaient permettre de rapprocher les informations à l'aide de

---

[87] Compte rendu du débat au Sénat français de la Séance du 17 novembre 1977, p. 2753.

[88] Roseline LETTERON, *L'administré et le droit à l'information,* thèse de doctorat, Paris, U.F.R. de Sciences juridiques, administratives et politiques, Université de Paris X, 1987, p. 108.
L'auteur souligne que « l'intérêt du Rapport Tricot réside, en premier lieu, dans un postulat de transparence des données nominatives contenues dans les fichiers ».

[89] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 75, p. 56.

[90] *Id.*

[91] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 75, p. 57.

traitements rendant l'opération possible, sans qu'il soit nécessaire qu'ils utilisent le même numéro d'identification.

Après l'analyse de ces questions, nous pouvons donc retenir du Rapport Tricot qu'il ne faut pas être obnubilé par l'interconnexion au sens technique du terme, mais plutôt travailler sur le plan des droits et obligations de ceux qui procèdent ou font procéder aux traitements informatisés.[92]

Ainsi, comme le Rapport Tricot nous le rappelle, c'est à l'instance de contrôle de décider, puisqu'elle aura dû connaître d'abord les questions relatives au traitement des renseignements personnels. Le rapporteur introduit ici les deux paramètres qui doivent servir à décider quelles informations peuvent être communiquées : le principe de finalité et le critère de la compatibilité. Le principe de finalité représente déjà à cette époque, l'élément clef permettant de déterminer comment doivent se réaliser les transmissions de données :

> « Elle appréciera si les communications prévues sont compatibles avec le respect des secrets légalement protégés et avec celui du principe de finalité que la commission propose d'inscrire dans la loi. Dans la mesure où cette compatibilité sera assurée, les communications seront en principe légitimes. »[93]

La légitimité des communications trouve donc son origine dans le contenu du principe de finalité et dans le degré de compatibilité que l'on devra apprécier au cas par cas. Cette tâche, nous le verrons plus tard, est loin d'être facile et pose des questions majeures si on parle d'un système en réseau où l'information circule davantage, et non de communications isolées et très concrètes dans un système en silo.

Le Rapport Tricot souligne, dans le cas des fichiers publics, l'importance du règlement par un acte juridique des questions relatives aux libertés que peut poser le recours aux moyens informatiques. De cette façon, l'acte juridique, précédant la

---

[92] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 75, p. 58.

[93] *Id.*, p. 59.

mise en place d'un traitement informatique, doit définir l'objet du traitement, sa finalité et prévoir si des interconnexions automatisées pourront être opérées avec d'autres fichiers[94].

Cette règle générale trouve des exceptions dans les actes relatifs aux fichiers concernant la sûreté de l'État et la sûreté publique, pouvant ordinairement être moins détaillés que les autres. Pour ce qui est des fichiers publics, les rapporteurs proposent de publier ces actes de création après soumission à l'instance de contrôle et, s'il y a lieu, au Conseil d'État.

Le principe de finalité, même avant l'adoption de la Loi I et L, a fait l'objet de réflexions et de débats : « La notion de finalité qu'on a vu apparaître au sujet de l'enregistrement et de la conservation des données se manifeste aussi quant à leur traitement, leur circulation et leur destination »[95].

Ce critère va déterminer tout le cycle de vie de l'information, du renseignement personnel et cela même au sein de l'appareil d'État où les informations doivent circuler sauf quand des exceptions et limites sont nécessaires.[96]

Le Rapport Tricot, pour ce qui est des traitements publics informatisés, établit que l'acte juridique de leur création va devoir indiquer quels sont les destinataires de chaque catégorie d'information, à l'intérieur même de la collectivité publique intéressée comme en dehors de celle-ci.

De même, si des réformes législatives ou administratives justifient que de tels fichiers soient transférés entièrement ou en partie à des tiers, un texte, de la même forme que l'acte de création du traitement, doit décider des précautions nécessaires, et cela dans un souci d'aider le fonctionnaire à savoir quand les renseignements personnels doivent ou non sortir de leur service. En 1975 en effet, le Rapport explique encore que : « dans le doute, les fonctionnaires ont tendance à opter pour la rétention de l'information. »[97]

---

[94] *Id.*, p. 32.
[95] *Id.*, p. 53.
[96] *Id.*
[97] *Id.*

Nous pouvons nous demander si cette réalité existe encore aujourd'hui et si, grâce au développement du gouvernement électronique, cette réalité va changer afin que les fonctionnaires connaissent parfaitement les destinataires des informations et sachent comment partager ces renseignements de façon à respecter les lois en la matière.

Qu'il s'agisse de fichiers publics ou privés, les rapporteurs soulignent le risque que ces informations puissent être détournées de leur finalité « du fait de l'exercice par des autorités publiques de certaines prérogatives en fait de contrôle ou de répression »[98]. Ce rapport ne donne pas de réponses ou de solutions à cette problématique, et explique que la Commission qui a rédigé le rapport n'a pas réussi à élaborer des propositions en la matière.

**B - Informatique et Libertés**

Lors de la discussion du Projet de Loi I et L au Sénat français, certains intervenants remarquent que le plus grand des dangers que cette loi veut éviter est le fait de pouvoir facilement rapprocher toutes les informations concernant les citoyens :

> « (…) tout est inscrit, répertorié, inventorié, absolument tout et avec cela une mémoire prodigieuse qui n'oublie jamais. Pourquoi tout cela ? Pour faire les opérations les plus complexes, mille et mille comparaisons, mille et mille rapprochements, grâce aux interconnexions. »[99]

La crainte, à cette époque, concerne cette capacité de rassembler les données personnelles touchant à un individu par la transmission des informations. Cette possibilité fait naître une préoccupation qui est prise en considération à l'heure de légiférer en la matière :

---

[98] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 75, p. 54.

[99] Compte rendu du débat au Sénat français de la séance du 17 novembre 1977, p. 2753 (nous soulignons).

> « Chacun de nous peut mesurer aujourd'hui, le danger qu'il y a à transmettre les informations à d'autres que ceux à qui elles ont été données. Toute personne est propriétaire des informations qu'elle communique ; elle donne, le cas échéant, un accord pour une utilisation déterminée : mais, au mépris de cet accord pour base, peuvent se produire des extensions considérables, prodigieuses. C'est un véritable trafic d'informations auquel il faut s'opposer. »[100]

À ce moment, les experts commencent à comprendre la problématique entourant la transmission des informations à des tiers et le sentiment de rejet à l'encontre de telles pratiques semble être au cœur des discussions entourant le projet de loi. Toujours lors d'une séance au Sénat, nous constatons une volonté de limiter ces pratiques : « Il faut maîtriser la machine afin qu'elle serve les hommes et la société »[101].

Et les intervenants fournissent déjà la formule qui peut très clairement servir à limiter les abus provoqués par l'utilisation de l'informatique :

> « C'est au moment de la collecte qu'il faut intervenir. Les questions sans rapport avec la finalité d'une enquête doivent être évitées. Il ne doit pas y avoir de buts cachés. » [102]

Dès lors, nous pouvons comprendre quelle est la volonté des législateurs à l'origine du principe de finalité, établissant déjà les limites au moment de la collecte des informations. Ainsi, les principes essentiels quant à l'utilisation des données personnelles sont identifiés très tôt dans l'élaboration de la loi française :

> « Un autre principe concerne la circulation des données. Les informations doivent être utilisées pour ce à quoi elles ont été collectées, et pour cela seulement. (…) Il faut interdire le détournement d'informations, la tricherie. Il faut empêcher que des collectes faites pour une chose servent à une autre chose : sinon, c'est l'abus, l'anarchie. »[103]

---

[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*

En effet, juste avant l'adoption de la Loi I et L, il nous est rappelé l'impact de projets visant à rapprocher des fichiers informatiques au sein du secteur public en France :

> « Le cours des événements allait être quelque peu influencé para la naissance, au début de 1974, d'un certain nombre de projets, dont le plus connu, dénommé S.A.F.A.R.I., visait à utiliser un identifiant unique – le numéro national d'identité, plus connu sous le nom de sécurité sociale – pour l'ensemble des répertoires et fichiers publics. La presse et l'opinion s'émurent. M. Pierre Messmer, alors Premier ministre, interdit aux services de procéder sans son autorisation à de nouvelles connexions de fichiers et demanda au Garde des sceaux de constituer une commission chargée de proposer un ensemble de mesures. »[104]

Bien sûr, la question de l'identification de tous les citoyens grâce à un numéro national d'identité a provoqué une crainte spécifique : « Et l'on sait l'émotion qu'a suscité naguère le projet baptisé – de façon quelque peu provocante – S.A.F.A.R.I. (…) qui devait permettre à partir du répertoire national d'identification des personnes physiques, de faciliter les intercommunications entre les fichiers qui auraient recours au numéro national d'identité, soit comme base de classement, soit comme élément de référence »[105].

Dans le Rapport présenté à l'Assemblée nationale par le député Jean Foyer nous pouvons lire quelles étaient les craintes concernant l'échange d'informations entre les différentes administrations, après le choc provoqué par le projet S.A.F.A.R.I. : « Une circulation trop fluide des informations entre les différents services de l'Administration abattrait d'utiles barrières et conférerait à tout fonctionnaire détenteur d'une parcelle de la puissance publique des pouvoirs excessifs »[106].
L'idée la plus répandue à cette époque juste avant l'adoption de la Loi I et L, est la crainte face à cette hyper-puissance des pouvoirs publics, à cause du contrôle des citoyens par la possession de leurs données personnelles. Le rapporteur précise encore :

---

[104] Rapport de M. FOYER, au nom de la commission des lois : Doc. Ass. Nat. n. 3125 du 4-10-1977, p. 12.
[105] *Id.*, p. 7.
[106] *Id.*

> « Sans être livré sur ce sujet à un effort de réflexion aussi poussé, le public éprouve un sentiment prononcé de défiance à l'égard d'un système automatisé qui, de façon très impersonnelle, va réunir un certain nombre de renseignements touchant à sa vie privée et qui seront ensuite aisément accessibles à un grand nombre d'utilisateurs dont certains, en l'état actuel du droit, ne sont même pas assujettis à l'obligation du secret professionnel. »[107]

Le rapport fait également part du sentiment de défiance à l'égard des traitements informatiques et, plus particulièrement, à l'égard des interconnexions entre les fichiers, phénomène nouveau et qui n'existait pas dans l'univers papier :

> « Certes, le phénomène n'est pas nouveau et la mise en fiches n'a jamais eu bonne presse dans l'opinion publique. Mais les fichiers manuels sont par nature peu maniables, disséminés et dotés d'un contenu hétérogène, ce qui empêche le traitement aisé des données collectées et leurs interconnexions. »[108]

Il nous semble décisif pour nos recherches en ce qui concerne la volonté du législateur de citer une partie d'un Rapport présenté par le sénateur Jacques Thyraud en 1977.

À cette occasion, le rapporteur, dans la partie relative à l'examen des articles de la Loi I et L, fait mention de la définition de « traitement automatique d'information », appellation présente dans ce texte, et il souligne cette idée – qui nous aide notamment à comprendre quel était l'objectif à l'heure de légiférer en la matière :

> « Il assimile notamment à un traitement l'interconnexion des fichiers, perspective qui, on le sait, a été à la base d'un vaste mouvement en 1974 et, à vrai dire, le véritable point de départ de la législation qui nous est soumise aujourd'hui. »[109]

Le Rapport Thyraud nous rappelle effectivement que le chroniqueur judiciaire du journal *Le Monde* avait alors écrit un article particulièrement percutant qui avait

---

[107] *Id.*
[108] *Id.* (nous soulignons).
[109] Rapport de M. J. THYRAUD, au nom de la commission des lois : Doc. Sénat n. 72 du 10-11-1977, p. 24 (nous soulignons).

motivé un grand sentiment de rejet à l'encontre du phénomène de l'interconnexion des fichiers. Nous voyons que, en effet, cette notion d'interconnexion en tant qu'assimilable à un traitement, est le point de départ de la législation en la matière, qui a eu comme base le principe de finalité.

Ce Rapport signale que le problème de ficher les individus et de rassemblement sur chacun d'eux d'un certain nombre d'informations susceptibles de porter atteinte à leur vie privée n'est pas nouveau, puisque l'existence de fichiers ne date pas d'aujourd'hui[110]. Toutefois, le rapporteur nous rappelle que l'informatique permet une rapidité de rassemblement des informations exceptionnelles et qu'elle apporte essentiellement un changement de dimension : « elle a introduit, en effet, une capacité de mémorisation considérable au point que certains peuvent craindre qu'elle ne porte atteinte à l'un des droits les plus fondamentaux de l'être humain : le droit à l'oubli »[111].

En 1977, les experts affirment que le danger le plus évident dérivant de l'informatique est la faculté de créer des profils grâce à la possibilité de réunir la totalité des informations concernant une personne et la capacité de stocker l'information pour toujours, grâce à la « mémoire totale » des ordinateurs.
Ils déterminent également quels sont – à cette époque et encore aujourd'hui – les vrais problèmes que pose le traitement automatisé des informations comme étant « des problèmes de collecte des données et d'utilisation de ces données »[112].

Particulièrement essentielle à nos recherches, la mention que le rapporteur fait quant à la doctrine du Conseil d'État en 1977 est tout à fait pertinente en ce qui concerne les questions reliées à l'informatique qui ont motivé l'adoption de la loi française en la matière :

[110] *Id.*, p. 6.
[111] *Id.*
[112] *Id.*, p. 8.

> « (…) Très récemment, le Conseil d'État a même été plus loin. Il a jugé que le fait de communiquer des informations personnelles à d'autres personnes que les fonctionnaires chargés d'exécuter la mission de service public qui requiert la constitution d'un fichier, faisait perdre à un tel fichier son caractère de document d'ordre intérieur. Dès lors, tout intéressé était "recevable à demander à connaître les mentions le concernant, à en contester l'exactitude et à en obtenir, le cas échéant, la suppression". »[113]

Il nous semble très pertinent de souligner que le rapporteur juge nécessaire de faire mention de cette doctrine du Conseil d'État. Et cela, parce que dans le passé comme au présent, la question de la transmission des informations peut avoir des conséquences majeures quant à la protection qui doit être accordée aux données personnelles qui font l'objet d'une communication.

Dans le passé, et plus particulièrement au moment de l'adoption de la Loi I et L, l'idée est que si l'information « ne bouge pas », si elle est statique, la protection des personnes est plus facile à garantir. Cette fois, c'est lors des débats à l'Assemblée nationale que nous retrouvons cette idée :

> « Au surplus – et c'est la vérité d'expérience – la liberté et la tranquillité du citoyen reposent, pour une part qui n'est pas négligeable, sur le cloisonnement des administrations et le peu de goût que celles-ci ont à l'ordinaire pour se communiquer les données qu'elles détiennent comme des trésors précieux. L'informatique, par le moyen des interconnexions, rend fluide et automatique la circulation des informations. »[114]

Notons d'abord que le cloisonnement, qui existe depuis toujours, des informations détenues par les différentes administrations et l'impossibilité d'interconnecter les informations de l'univers papier semblait être une source de tranquillité pour les citoyens et les pouvoirs publics avant la venue de l'informatique.
L'habitude de retenir les informations, croyant que la détention de l'information représente l'exercice du pouvoir, et l'impossibilité technique de faire circuler les

[113] *Id.*, p. 9.
[114] Compte-rendu du débat à l'Assemblée nationale de la Première séance du 4 octobre 1977, p. 5782 (nous soulignons).

informations entre les différents services de l'administration servaient à maintenir le cloisonnement des informations, ce qui empêchait le croisement des données personnelles.

Pour cette raison, la figure de l'interconnexion est perçue de façon très négative et symbolise la fin d'une certaine tranquillité puisque, normalement, les informations ne circulent pas. Pour résumer un tel sentiment : « Jusqu'à présent ces données étaient éparses. Désormais elles pourront être concentrées, puisque l'utilisation de l'informatique permet des recoupements et c'est une source de risques »[115].
L'auteur américain A.L. Newman nous rappelle que la volonté était à l'époque de « centraliser » les informations, tout en recherchant une plus grande efficacité des services :

> « *With the proliferation of computer technology in large organizations, goverments proposed linking previously discrete information from diverse collection points. The goal of such efforts was to enhance efficiency and oversight of growing public and businness services*. »[116]

Cette idée nous aide à comprendre que ces lois « de première génération » étaient conçues pour encadrer une administration « en silo » et que le législateur voulait garder ce modèle, comme étant le seul capable de protéger les informations concernant les citoyens.
C'est pourquoi, les principes que ces lois imposent ont du mal à protéger les renseignements personnels dans un modèle d'administration en réseau, où les informations doivent circuler à tout moment afin d'offrir aux citoyens un service de qualité. Dans les pages qui suivent, nous aurons l'occasion de comprendre dans quelle mesure ce changement a un grand impact sur la façon dont on va protéger les renseignements personnels dans le contexte du gouvernement électronique, modèle réseautique par excellence.

---

[115] *Id*., p. 5788.
[116] Abraham L. NEWMAN, *Protectors of Privacy, Regulating Personal Data in the Global Economy*, Ithaca, Cornell University Press, 2008, p. 45 et 46.

Pour essayer d'encadrer l'utilisation de l'informatique et de maîtriser les risques provenant de son utilisation, le projet de loi français, qui est devenu, une fois approuvé, la Loi I et L, apporte une solution :

> « Il énonce donc des principes, des principes seulement, car nous sommes là dans un domaine qui évolue très vite. Si nous voulions entrer dans trop de détails, l'évolution des techniques aboutirait à rendre vite caduques les règles trop précises que nous aurions voulu adopter. Nous abordons un terrain qui est encore en friche et presque inconnu. Il serait déraisonnable de prétendre organiser en détail un domaine aussi nouveau. L'informatique est promise à un développement très rapide, qui dans une assez large mesure, est imprévisible, comme l'est la recherche scientifique elle-même. Par conséquent, la loi que nous vous proposons a un caractère expérimental. »[117]

Ces débats à l'Assemblée servent à comprendre quelle était la volonté du législateur qui a voulu essayer de maîtriser les risques grâce à une loi qui énonce, essentiellement, des principes, cela à cause de la spécificité de la technologie que le législateur voulait encadrer, changeante et évolutive par nature. Voici pourquoi cette loi est fondamentalement articulée par des principes et non par des règles, trop précises et fermées.

Cependant, au moment de se référer aux limites juridiques à l'enregistrement des données, les rapporteurs soulignent cette idée, qui représente l'esprit du rapport Tricot en ce qui concerne la finalité : « Sur le plan du droit également, l'adéquation des données à la finalité doit être une idée directrice, plus féconde, croyons-nous, que les interdictions a priori »[118].

C'est ainsi que ce principe devient essentiel, comme l'idée directrice capable d'éviter les interdictions *a priori* et visant à servir d'élément essentiel pour déterminer l'adéquation des traitements à la finalité déclarée.

---

[117] Compte-rendu du débat à l'Assemblée Nationale de la Première séance du 4 octobre 1977, p. 5789 (nous soulignons).

[118] COMMISSION NATIONALE DE L' INFORMATIQUE ET DES LIBERTÉS, préc., note 75, p. 46.

## SECTION 2 Principe de finalité, l'État en réseau et administration électronique

Nous analyserons, dans les pages qui suivent, les conditions de circulation des informations que le gouvernement ou l'administration électronique impose, mais aussi les conséquences du passage d'un État en silo à un État en réseau, pour, par la suite, identifier les défis qui se présentent pour la gouvernance visant à protéger la vie privée des citoyens.

Finalement, nous étudierons la manière dont se réalise le passage d'un modèle d'État à un autre et le rôle que le principe de finalité va devoir jouer dans l'encadrement de la circulation des renseignements personnels.

### 1- L'État en réseau et l'administration électronique : vers la Prestation électronique des services

Notre recherche s'inscrit dans le contexte d'un modèle d'administration ou gouvernement en réseau venu remplacer le modèle classique d'administration en silo. Cette administration, qui est « électronique » en Europe, est également un « Gouvernement en direct », un « Gouvernement en ligne » ou un « Gouvernement électronique » au Canada. Selon certains, ces termes s'utilisent indifféremment pour désigner cette notion, ils ne s'opposent pas mais se complètent[119].

Ces différents termes désignent un nouveau modèle qui a pour objectif d'établir une administration plus axée sur les rapports avec les citoyens et cela grâce à l'utilisation des nouvelles technologies de l'information et de la communication. L'« administration en ligne » est définie comme l'ensemble des services gouvernementaux accessibles par l'intermédiaire d'Internet[120].

---

[119] Karim BENYEKHLEF, « L'administration publique en ligne au Canada : précisions terminologiques et état de la réflexion », (2004) *Revue française d'administration publique* n° 110, 267, 269.

[120] Définition fournie par le Grand dictionnaire terminologique de l'Office québécois de la langue française.

Des précisions terminologiques s'imposent toutefois, comme certains l'ont souligné, « (…) la notion d'*administration*, lorsqu'elle est électronique, ne semble pas se référer uniquement à la sphère gouvernementale proprement dite, mais également les termes de *gouvernement en ligne* ou de *cybergouvernement* sont employés dans des contextes similaires »[121].

Il nous faut comprendre pour quelle raison ce nouveau modèle d'administration présente des enjeux majeurs en ce qui concerne la protection des renseignements personnels circulant dans les bases de données de l'appareil étatique, ce qui va nous servir pour identifier clairement pourquoi l'application du principe de finalité dans ce contexte est une question intéressante.

Le rapport de Thierry Carcenac introduit la notion en 2000[122] en présentant un modèle « d'administration électronique citoyenne »[123] qui présente la question sous le point de vue des rapports entre les citoyens et l'État, et en affirmant qu'« Internet doit être mis au service de la réforme de l'État et, notamment, au service des agents au contact des citoyens »[124].

Les auteurs d'un tel rapport préconisent déjà la facilitation du passage « d'une administration proposant des services *en silo* vers une administration proposant des services en réseau »[125], ce qui va impliquer nécessairement « une fluidité de la circulation des données dans les systèmes d'information de l'État »[126]. Et cela, afin de « rendre disponibles les informations aux différents intervenants par la mise en réseau de l'administration »[127], ce qui aura évidemment des conséquences majeures pour ce qui est de l'encadrement de ce nouveau modèle de circulation des renseignements personnels.

---

[121] Karim BENYEKHLEF, préc., note 119, 269.
[122] Voir sur l'historique du concept : Patrice FLICHY et Éric DAGIRAL, « L'administration électronique : une difficile mise en cohérence des acteurs », (2004) *Revue française d'administration publique* n° 110, p. 245, 247.
[123] Thierry CARCENAC, *Pour une administration électronique citoyenne - méthodes et moyens*, Paris, La Documentation française, 2000.
[124] *Id.*, p. 12.
[125] *Id.*, p. 14.
[126] *Id.*, p. 17.
[127] *Id.*, p. 56.

Le Rapport « Administration électronique et protection des données personnelles »[128] a contribué, en 2002, à mieux cerner les enjeux que ce nouveau modèle d'administration présente pour ce qui est de la protection de la vie privée du citoyen. Le rapport présente cette administration :

> « L'usager est aujourd'hui confronté à une administration cloisonnée, chaque administration posant les mêmes questions, demandant les mêmes pièces justificatives. L'*interface unique* devrait permettre à l'usager de communiquer certaines données à une administration, à charge pour celle-ci de les faire suivre à d'autres. Tout cela suppose que les administrations collaborent, et, le cas échéant, échangent des données entre elles. »[129]

En effet, ce modèle d'administration électronique suppose une circulation accrue des informations, ainsi que des échanges de données entre les différentes administrations.

Voici le modèle qui représente ce changement de paradigme :

> « L'administration électronique suppose la circulation accrue d'informations. Le déroulement en réseau de plusieurs des activités inhérentes aux fonctions de l'État comporte plusieurs avantages. Il favorise une organisation centrée sur le citoyen ou l'usager ; il facilite la collaboration et le travail coopératif entre une pluralité d'acteurs de statuts différents. Il facilite la spécialisation flexible se fondant sur l'échange entre des pôles interagissant. »[130]

Ce modèle se caractérise par une circulation fluide des informations et par des échanges constants. Ce modèle de « Gouvernement en direct, entre autres avantages, simplifiera la prestation des services, facilitera l'accès aux services et aux renseignements gouvernementaux et éliminera les dédoublements »[131].

---

[128] Pierre TRUCHE, Jean-Paul FAUGÈRE, Patrice FLICHY, *Administration électronique et protection des données personnelles - Livre blanc*, Paris, La Documentation française, 2002.
[129] *Id.*, p. 7.
[130] Pierre TRUDEL, « Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles », (2004) *Revue française d'administration publique* n° 110, p. 257, 258.
[131] COMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Allocution présentée par C. BEAULÉ au *Groupe de travail interministériel sur la vie privée et le*

Nous ne pouvons pas procéder dans le cadre de cette recherche à l'examen en profondeur toutes les questions relatives à l'administration électronique. Toutefois, il nous semble important de définir en quoi la mise en place de celle-ci peut avoir des conséquences pour ce qui est du droit à la protection de la vie privée.

Pour certains, dans le contexte québécois, le « gouvernement en ligne » se définit par trois composantes[132] : l'Administration électronique, qui vise l'amélioration de l'ensemble des processus administratifs internes et externes du gouvernement, et où l'on trouve les services en ligne qui cherchent spécifiquement à améliorer de processus de prestation de services auprès du citoyen ; la Cyberdémocratie, qui a pour but le développement et l'amélioration des relations avec le citoyen en tant qu'acteur politique ainsi que les relations gouvernementales ; la Société de l'information, qui a pour objectif le développement et l'amélioration des relations sociales avec l'ensemble des parties prenantes de la société civile.

Trois grands domaines du Gouvernement en ligne ont été identifiés par certains experts : la « e-administration », la « e-démocratie » et la « e-société », qui ne sont pas mutuellement exclusifs, même si chaque domaine nous permet de distinguer différents projets[133].
Pour d'autres, les trois composantes de « l'idée générale de la mise en ligne des administrations sont l'administration électronique (prestations de services aux citoyens), le gouvernement en ligne (optimisation de la gouvernance démocratique) et la démocratie en ligne (participation et consultation en ligne des citoyens) »[134].

Dans le cadre de nos recherches, l'administration électronique est la composante qui présente les enjeux majeurs pour ce qui est de la protection des renseignements

---

*Gouvernement en direct*, Ottawa, Ontario, 8 mai 2002, en ligne : "http://www.priv.gc.ca/speech/02_05_a_020508_f.cfm" (consulté le 14 mai 2011).

[132] Cette définition est celle que nous retrouvons dans le site des Services Gouvernementaux du Gouvernement du Québec : http://www.msg.gouv.qc.ca/gel/index.html.

[133] Gilles ST-AMANT, « E-Gouvernement : cadre d'évolution de l'administration électronique », (2005), *Revue Systèmes d'information et Management*, n° 1, vol. 10, 16 et 17.

[134] K. BENYEKHLEF, préc., note 119, 272.

personnels. C'est dans ce domaine que nous retrouvons le « e-service qui vise spécifiquement l'amélioration des processus de prestation de services avec le citoyen »[135] et que « l'accent ainsi mis sur l'efficience des services se manifeste *via* la circulation et le partage de l'information »[136].

Pour certains, un des facteurs d'amélioration de la qualité de production des administrations provient du décloisonnement des administrations, puisque « l'application de nombreuses règles juridiques nécessite la connaissance d'informations détenues par d'autres institutions »[137].

Ce modèle est basé sur le déploiement de téléprocédures ou plutôt téléservices, mettant l'accent sur le service que l'administration cherche à rendre[138]. Il a été dit que le terme de « téléprocédure » recouvre plusieurs acceptions dont l'objectif ultime est de parvenir à supprimer totalement la phase « papier ». Elle a été définie comme un « échange dématérialisé de formalités entre une autorité publique et ses partenaires et usagers »[139].

C'est en effet, dans le contexte de cette administration électronique, que les téléprocédures, les téléservices en Europe ou les « Grappes de services » au Québec, en tant que « regroupements de services intégrés, ayant un lien naturel, que l'on peut obtenir en ligne et en une seule opération, à partir d'un portail, qui est mis en place afin de simplifier les démarches des citoyens et de rendre plus directe la prestation de services »[140], se déroulent.

La mise en place de ces grappes de services s'appuie normalement sur un guichet unique et, selon la définition du Grand dictionnaire terminologique de l'Office

---

[135] Gilles ST-AMANT, préc., note 133, 17.
[136] K. BENYEKHLEF, préc., note 119, 269.
[137] Jacques SAURET, « Efficacité de l'administration électronique et service à l'administré : les enjeux de l'administration électronique », (2004) *Revue française d'administration publique* n° 110, 279, 281.
[138] P. TRUCHE, J.-P. FAUGÈRE, P. FLICHY, préc., note 128, p. 29. Ce rapport considère que la notion de téléprocédure est datée et préfère celle de téléservice à être utilisée dans le contexte de l'administration électronique.
[139] T. CARCENAC, préc., note123, p. 130.
[140] Définition fournie par le Grand dictionnaire terminologique de l'Office québécois de la langue française.

québécois de la langue française, « permet d'éviter à l'usager de subir les désagréments dus aux cloisonnements entre les administrations et même au sein de celles-ci ».

Voici la façon dont s'organisent les grappes de services au Québec, dans le cadre du gouvernement en ligne :

> « La circulation de l'information entre administrations doit être organisée afin de réduire les formalités pour les usagers lorsqu'un événement de la vie nécessite d'informer différentes administrations. Pour faciliter la recherche aux citoyens, on structure l'information en grappes, qu'elle soit intra- ou interministérielle, voire même intergouvernementale, de façon à ce que les internautes trouvent tous les renseignements relatifs à un même sujet au même endroit. »[141]

La Prestation électronique de services est une prestation de services gouvernementaux, sécurisés ou non, offerts aux citoyens par l'intermédiaire d'Internet[142]. Les professeurs V. Gautrais et P. Trudel utilisent l'expression de « prestations en ligne » pour faire référence aux services gouvernementaux qui nécessitent une « circulation » des renseignements personnels et qui peuvent prendre des formes particulièrement variées[143].

Pour ces auteurs, les prestations en ligne constituent la couche de services qui permet de mettre en relation les citoyens et les diverses entités de l'Administration :

> « Les prestations en ligne au sein d'un réseau se présentent comme des processus assurant des prestations pouvant concerner une pluralité d'entités, de ministères ou organismes publics. Ce sont des services qui, au sein d'un réseau procurent des interfaces de même que

---

[141] Extrait de la Note accompagnant la définition de « Grappe de services » fournie par le Grand dictionnaire terminologique de l'Office québécois de la langue française. Ce dictionnaire signale également que le gouvernement en ligne peut développer des grappes de services pour les différentes étapes qui rythment la vie des citoyens : une naissance, un mariage, un changement d'adresse, un changement lié à l'emploi, etc.

[142] Définition fournie par le Grand dictionnaire terminologique de l'Office québécois de la langue française. La note accompagnant cette définition signale qu'effectuer un changement d'adresse en ligne, demander ou renouveler un permis ou une carte, remplir ou acheminer un formulaire en ligne, donner son opinion lors de consultations publiques sont des exemples de services gouvernementaux accessibles par Internet.

[143] Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010.

> diverses fonctions afin de soutenir les échanges et partages d'informations. »[144]

Ainsi, ces prestations en ligne procurent-elles des « passerelles » visant à assurer la disponibilité des informations nécessaires à leur réalisation pour le bénéfice des « citoyens-usagers ». Il faut noter que ces passerelles « que constituent les prestations en ligne se présentent alors avec les caractéristiques des interfaces et des infrastructures de réseaux »[145]. Pour ces auteurs, l'avènement des services en ligne requiert une circulation accrue et le partage des informations, ce qui permet d'améliorer la qualité et la célérité des prestations[146]. En plus, « les prestations en ligne qui se développent dans la plupart des administrations publiques supposent le déploiement de services en ligne emblématiques des modes de circulation de l'information qui émergent désormais au sein des réseaux »[147].

L'administration électronique qui est au centre de nos travaux de recherche est celle qui se caractérise par sa forme de réseau, par une circulation accrue des informations et par un partage permettant d'offrir des prestations électroniques de services aux citoyens. Dans le cadre de cette administration électronique, nous identifions la prestation électronique des services comme l'élément central définissant les nouveaux rapports État-citoyen et pouvant donner lieu à une augmentation des échanges d'informations entre les différents organismes du secteur public.

C'est dans ce nouveau contexte que les enjeux relatifs à l'encadrement de la protection des renseignements personnels dans ce nouveau modèle d'administration seront étudiés dans les pages qui suivent.

---

[144] *Id.*, p. 14.
[145] *Id.*, p. 14.
[146] *Id.*, p. 15.
[147] *Id.*, p. 17.

**2- Finalité face aux impératifs de l'administration électronique**

Dans le contexte de la protection des renseignements personnels dans le secteur public, nous assistons depuis quelques années à la mise en place d'un nouveau modèle de circulation des informations, qui nous oblige à reconsidérer la pertinence de la formulation des principes de protection des textes législatifs qui ont vu le jour à partir de la fin des années 1970. Un nouveau modèle d'État, qui prend la forme d'un réseau[148], provoque un changement majeur dans les modalités de circulation des informations concernant les citoyens.

Il est important de souligner que le principe de finalité est le seul capable de limiter la réutilisation des informations concernant les citoyens dans le cadre de la mise en place du gouvernement électronique et dans celui de l'offre de la prestation électronique de services. Nous aurons l'occasion, dans nos travaux, d'approfondir la manière dont la jurisprudence de la CNIL agit pragmatiquement à l'heure de se pencher sur le principe de l'extension de finalité.

La CNIL a fait preuve d'une grande sévérité au moment d'accorder ces extensions de finalité, mais, comme cela a déjà été dit, il n'est pas certain que cette politique de rigueur se perpétue : « pour certains, elle peut compromettre les chances de réussite d'une réforme administrative qui passe par une meilleure circulation de l'information »[149].

Comme dit précédemment, « la tentation est grande, en effet, de ne pas refaire le travail qui a été effectué par d'autres et de rentabiliser les gisements de données qui ont déjà été collectées à d'autres fins »[150]. Nous sommes ici devant la question de l'extension de la finalité qui va encadrer un certain rapprochement ou rassemblement des informations, puisque « la tendance, en effet, est à

---

[148] Pierre TRUDEL, *État de droit et effectivité de la protection de la vie privée dans les réseaux du e-gouvernement*, Communication présentée lors du colloque national « Technologies, vie privée et justice », tenu à Toronto par l'Institut canadien d'administration de la justice (ICAJ) du 28 au 30 septembre 2005, p. 13, en ligne : http://www.chairelrwilson.ca **(**consulté le 12 mars 2011).
P. Trudel a défini le concept des réseaux comme étant des « *environnements interconnectés dans lesquels l'information circule dans pôle à l'autre, de façon multidirectionnelle et non hiérarchique* **».**

[149] Voir sur les différents points de vue entourant cette question : C. MARLIAC-NÉGRIER, préc., note 43, p. 461.

[150] F. LESAULNIER, préc., note 57, p. 216.

l'allongement des délais de conservation et à l'admission des réutilisations des données »[151]. Toutefois, alors que la longévité des données croît, « les délais d'accès aux données s'amenuisent et nombre de traitements ultérieurs sont considérés comme compatibles avec les finalités initiales »[152].

Il est clair que le phénomène de la mise en place de l'administration électronique va supposer une réforme totale du modèle classique d'administration et, plus particulièrement, des modes de circulation des informations au sein de l'appareil étatique. Il sera intéressant de voir comment la rigidité d'aujourd'hui, à l'heure de décider de l'approbation d'une extension de finalité d'un traitement, va devoir s'adapter aux besoins provenant d'une éventuelle « réutilisation » de l'information aux mains de l'État pour répondre aux modes de fonctionnement de l'administration électronique.

En 2001 déjà, certains pensaient que « nous devons faciliter le passage d'une administration proposant des services en silo vers une administration proposant des services en réseau »[153]. Ch. Boudreau attire notre attention sur cette transformation de l'État et sur les nouveaux modes de gestion qui se développent afin de répondre à ce modèle :

> « Dans cette économie dominée par l'innovation et la compétitivité, l'organisation y compris l'État, doit plus que jamais être innovante et, pour ce faire, s'organiser en réseau plutôt qu'en silo. Cela ne signifie pas pour autant la disparition de l'organisation bureaucratique. D'autres modes de gestion plus horizontaux et plus flexibles doivent se superposer aux hiérarchies actuelles afin de répondre plus adéquatement aux exigences des citoyens et des entreprises. »[154]

### A- Le partage d'informations

Suivant ce nouveau modèle, des « services gouvernementaux intégrés » ou des « prestations électroniques de services » seront offerts aux citoyens, impliquant

---

[151] *Id.*
[152] F. LESAULNIER, préc., note 57, p. 217.
[153] T. CARCENAC, préc., note 123, p. 12.
[154] Christian BOUDREAU, « À l'aube d'une transformation profonde de l'État », *Revue Télescope, Observatoire de l'administration publique de l'ENAP*, vol. 10, n° 5, novembre 2003, 2, 3 (nous soulignons).

éventuellement de nombreux échanges de données entre organismes publics[155] et un plus grand nombre d'interconnexions des fichiers détenus par les administrations.

Devant cette transformation majeure, une partie de la doctrine se pose la question : « Est-ce que quelque chose doit changer dans la perception et l'énonciation du droit pour assurer la protection de la vie privée dans un univers de réseaux où l'information circule de plus en plus ? »[156].

Certains auteurs se demandent comment ces échanges seront encadrés dans le futur :

> « Les nouvelles modalités d'une circulation très fluide des informations sur le réseau peuvent-elles être régulées ? Est-il utopique ou non d'espérer que le citoyen pourra maîtriser l'utilisation de ses propres données et donner un contenu réel à la notion d'habeas data ? Parallèlement au mouvement en cours dans le secteur privé avec le commerce électronique, la portée et les conséquences de ces innovations dans les relations que le secteur public a avec ses usagers doivent être évaluées. »[157]

D'autres intervenants affirment que « les lacunes du droit traditionnel de la protection des données et la nécessité d'un changement de perspective sont manifestes »[158]. Par conséquent, « face à cela, se dessinent les contours encore imprécis d'un nouveau code de la circulation des données »[159]. Ce nouveau code complet de circulation des données devrait « dépasser la conception traditionnelle d'une protection des données unilatérale, à caractère purement défensif »[160].

---

[155] Edwin LAU, « Principaux enjeux de l'administration électronique dans les pays membres de l'OCDE », (2004) 110 *Revue française d'administration publique* 225, 228.

[156] Vincent GAUTRAIS, « Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle », *Revue Lex Electronica*, vol. 9, n° 2, Numéro Spécial, Été 2004, p. 2, en ligne : http://www.lex-electronica.org (consulté le 17 février 2011).

[157] Herbert MAISL, « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager », dans George CHATILLON et Bertrand DU MARAIS (dir.), *L'administration électronique au service des citoyens*, Bruxelles, Bruylant, 2003, 349, p. 352.

[158] Thomas WÜRTEMBERG et Gernot SYDOW, « Administration électronique et vie privée en Allemagne », dans George CHATILLON et Bertrand DU MARAIS (dir.), *L'administration électronique au service des citoyens*, Bruxelles, Bruylant, 2003, 361, p. 365.

[159] *Id.*

[160] *Id.*

Cela fait penser à l'idée du droit « négocié », qui s'adapte parfaitement à cette nouvelle conception du droit relatif à la protection des renseignements personnels avancé par une partie de la doctrine.

Certains auteurs proposent également une démarche partant de l'information nominative conçue comme objet de devoirs et de pouvoirs, ce qui permet un rééquilibrage des questions, tout en dépassant une certaine étroitesse propre à l'approche purement défensive de la protection « centrée sur la défense d'une zone irréductible de vie privée, pour vérifier que les menaces mettent aussi en cause l'identité, la réputation des personnes, mais aussi leur épanouissement personnel, objet d'une incontestable valorisation contemporaine »[161].

En effet, cette approche cède la place à une vision plus adaptée à aujourd'hui, plus réaliste avec la conciliation de la vie privée avec d'autres intérêts. On a souligné également l'importance de réévaluer certains principes fondamentaux des systèmes de protection des renseignements personnels tels que celui faisant référence à la finalité, ainsi que la nécessité d'introduire des nouveaux critères :

> « Il importe donc de repenser le droit de la vie privée en changeant le paradigme de suspicion vis-à-vis des gestionnaires des renseignements personnels et en introduisant des nouveaux critères fondateurs. En effet, et sans forcément bouleverser l'ensemble des principes, certains tels que la finalité, le consentement préalable systématique, la limitation de l'utilisation des renseignements personnels semblent peut-être devoir être réévalués. »[162]

Nous constatons, et nous aurons l'occasion d'analyser cela plus en profondeur, que des auteurs d'un côté comme de l'autre de l'Atlantique dénoncent les difficultés, pour le droit actuel relatif à la protection des renseignements personnels, de pouvoir encadrer de manière satisfaisante les nouveaux flux d'informations personnelles concernant les citoyens.

Effectivement, le partage d'informations sera nécessaire afin de pouvoir offrir au citoyen des prestations électroniques de services qui, dans le passé, se déroulaient dans le cadre de l'univers « papier » et où les citoyens étaient obligés de fournir des

---

[161] F. LESAULNIER, préc., note 57, p. 25.

[162] V. GAUTRAIS, préc., note 156, p. 9 (nous soulignons).

documents produits par un ensemble d'organismes publics de très différentes natures, appartenant parfois à l'administration fédérale, parfois à l'administration provinciale ou municipale[163].

Certains soulignent la manière dont un nombre infini d'informations sont traitées avec une très grande rapidité, en permettant, grâce à l'informatique, de faciliter les échanges d'informations, notamment dans le cadre de l'entraide administrative. C'est dans ce cas que d'aucuns parlent du « phénomène de la banalisation des données », phénomène relié sans doute, au respect du principe de finalité :

> « L'informatique, par rapport au traitement manuel, permet d'utiliser sans fin les données collectées et pour des buts différents souvent incompatibles avec le but initialement prévu. Sans limite, l'information pourrait circuler sans qu'on puisse savoir d'où elle provient et pour quel but elle a été originairement recueillie. Elle est en quelque sorte banalisée. »[164]

La CNIL soutient dès 2000 : « Soit, mais le problème est davantage celui du *silo* – c'est-à-dire le rassemblement dans une même base de données d'informations jusqu'à présent cantonnées en fonction d'une finalité définie avec précision – que celui de la mise en *réseaux* »[165].

### B- La multiplication des connexions

En effet, la question principale est la crainte de la naissance de risques provenant d'une « interconnexion généralisée des fichiers administratifs, d'un S.A.F.A.R.I.

---

[163] FORUM DES DROITS SUR L'INTERNET, *Conclusions dur le débat public « Administration publique et données personnelles »*, 2002, en ligne : http://www.foruminternet.org/publications/lire.phtml?id=476 (consulté le 15 avril 2010).
Comme le *Forum des droits sur Internet* le signale, nous allons pouvoir penser à l'instauration d'une nouvelle dynamique dans les rapports entre le citoyen et l'administration grâce à une réduction des contraintes imposées au citoyen, notamment en remplaçant l'obligation de pièces justificatives par un mécanisme de déclaration sur l'honneur.

[164] Jean-Philippe WALTER, *La protection de la personnalité lors du traitement de données à des fins statistiques*, Fribourg, Éditions Universitaires Fribourg-Suisse, 1988, p. 15 (nous soulignons).

[165] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *22 Rapport d'activité*, 2001, p. 109, en ligne: http://www.cnil.fr (consulté le 12 février 2011).

bis »[166]. Nous avons pu constater dans les pages précédentes que le projet S.A.F.A.R.I. a été à l'origine en France de la législation « Informatique et libertés » et de la réflexion visant à empêcher le croisement de l'ensemble des bases de données au sein de l'administration publique.

Pour quelques-uns, le phénomène de la généralisation d'un système d'identification basé sur des données biométriques pourrait renforcer encore davantage les modalités d'exercice du pouvoir de l'État sur les citoyens.

Or l'avènement de certains phénomènes peut aller à l'encontre des garanties reconnues par les premières législations en la matière :

> « L'équilibre né de la première loi Informatique et libertés de 1978 et des avis de la Commission Nationale de l'Informatique et des libertés (CNIL), notamment l'interdiction de l'interconnexion des fichiers informatiques et la limitation du recours à un identifiant unique, se trouve aussi gravement mis en cause. »[167]

L'apparition de certaines technologies dans le fonctionnement du nouveau modèle de l'État va également provoquer des questionnements touchant à des problématiques que nous avons cru résoudre par le passé.

La circulation en réseau des données personnelles peut certainement aider à offrir un service public de qualité aux citoyens, tout en évitant le détournement de la finalité des traitements : « La mise en réseau des fichiers d'administrés – dès lors qu'elle ne conduit pas à détourner leur traitement de sa finalité – est de nature à garantir la continuité du service rendu par les divers opérateurs administratifs avec lesquels ils sont en relation, dans des cas où la multiplication et la dispersion des saisies des informations sur papier peut mener à des incohérences – notamment lors

---

[166] *Id.* Nous pouvons donc constater que les problèmes peuvent, 20 ans après, se reproduire si des mesures adéquates ne sont pas adoptées.

[167] COLLECTIF D'AUTEURS (LIGUE DES DROITS DE L'HOMME, SYNDICAT DES AVOCATS DE FRANCE, et al.), *INES, de la suspicion au traçage généralisé*, dans *Traçage électronique et libertés*, Nathalie MALLET-POUJOL (dir.), *Problèmes politiques et sociaux n° 925*, Paris, La Documentation Française, 2006, p. 31.

des transmissions de dossiers en cas de changement de résidence, ou encore face à des demandes successives se rapportant à une même prestation »[168].

La mise en place de l'administration électronique et la modernisation de l'appareil étatique nous montrent que certains dangers ont vu le jour avec l'avènement de la circulation en réseau de certaines informations concernant les citoyens. Nous allons devoir faire face à la régulation de multiples interconnexions entre les différents ministères et organismes qui seront mis en place afin d'offrir des services aux citoyens via Internet.

Derrière le phénomène des interconnexions et l'indispensable respect du principe de finalité dans le contexte du secteur public, on peut lire : « Le champ des informations susceptibles d'être traitées pour une finalité donnée doit être clairement délimité, et les échanges d'informations ou les interconnexions de fichiers, dans le cadre de procédures répondant à des finalités distinctes, doivent être encadrés par les textes »[169].

La mise en réseau des informations, circulant sur Internet et sur l'Intranet des administrations, requiert un examen des modalités d'interconnexion. Nous pouvons identifier déjà certains risques auxquels nous allons devoir faire face dans le contexte qui nous occupe, notamment en ce qui concerne la création de profils des citoyens grâce au croisement d'informations ayant pour résultat une vision assez complète de tous les domaines de la vie de chaque citoyen (revenu, éducation, santé, etc.).

Ce partage d'informations devient nécessaire dans ce contexte, mais nous pouvons nous demander comment ce nouveau modèle sera mis en place, tout en respectant les lois de protection des renseignements personnels et, plus particulièrement, le principe de finalité.

Il faut noter que, même si aucun principe essentiel de protection des renseignements personnels n'interdit les interconnexions, le principe de finalité que les lois reconnaissent est celui qui empêche qu'une interconnexion généralisée des

[168] G. BRAIBANT, préc., note 56, p. 4.
[169] *Id.*, p. 9.

fichiers publics soit possible. Cependant, si nous analysons les enjeux relatifs aux interconnexions, l'étude du principe de finalité doit être placé au centre de l'analyse. Voici ce que la CNIL a signalé à cet effet :

> « Certes, aucun principe de protection des données personnelles n'interdit les interconnexions. Mais, le principe de finalité justifie les précautions particulières prises en matière d'interconnexions de fichiers ou de regroupements dans un même ensemble d'informations provenant de fichiers distincts. Ainsi, la plupart des législations de protection des données soumettent les interconnexions entre fichiers à des finalités différentes fussent-ils détenus dans le cadre d'une même administration, à un régime particulier de contrôle par l'autorité de protection des données. »[170]

Même si, dans le cas de la France, pour ce qui est du secteur public, les interconnexions ne sont pas interdites par principe, si elles ont été très encadrées et entourées de garanties, nous devons cependant noter que « cette sage prudence est quelquefois mal comprise de quelques administrations qui en déduisent que la CNIL est par principe hostile aux interconnexions entre fichiers »[171].

Dans la plupart des systèmes dotés d'une législation spécifique en matière de protection des renseignements personnels, les interconnexions entre fichiers publics font également l'objet d'une attention très particulière. Ainsi, la technique du « *data matching* » est utilisée afin d'établir, pour chaque interconnexion autorisée, un bilan coût-avantage qui sera généralement présenté à l'autorité de contrôle[172].

Selon certains, il serait raisonnable que l'administration utilise des renseignements pour des finalités qui peuvent nous sembler différentes de celles qui apparaissaient dans la déclaration du traitement en question. Ce qui peut justifier une telle utilisation, c'est que ces finalités sont « compatibles » ou « adéquates » aux

---

[170] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 165, p. 109 (nous soulignons).

[171] Voir à ce sujet : COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Les libertés, et l'informatique, Vingt ans de délibérations commentées*, Paris, La Documentation française, 1996, p. 170 et s.

[172] *Id.*

compétences administratives ou à la nature administrative de l'organisme en question[173].

Dans ce cas, nous parlons d'une utilisation différente (par rapport à leur finalité initiale) de certains renseignements, mais toujours utilisés par le même organisme ou ministère, ce qui déjà peut présenter *a priori* des garanties adéquates quant à la protection des renseignements personnels.

Prenons cependant le cas d'un scénario autre, qui ne serait pas celui qui se développe aujourd'hui : dans le cadre de la circulation des renseignements dans l'État en réseau, les renseignements sont utilisés par des organismes différents de celui qui avait recueilli les renseignements.

Même dans le premier cas (celui où un même organisme utilise les renseignements pour des usages que nous pouvons considérer comme compatibles), nous sommes en train de faire une présomption. Nous ne sommes pas toujours en mesure d'affirmer qu'un organisme a, parmi ses tâches, des activités qui vont impliquer l'utilisation de renseignements personnels qui vont toujours supposer une réutilisation à des fins compatibles.

Face à ce constat, nous sommes appelés à nous interroger sur la façon d'envisager un travail de recherche qui aurait pour but d'identifier les enjeux relatifs à la protection des renseignements personnels dans les environnements en réseaux et le pourquoi de l'inadaptation des lois en vigueur face à ce phénomène.

Si nous examinons les enjeux identifiés, nous pouvons affirmer qu'ils sont communs à l'ensemble des environnements en réseau et non seulement au contexte de l'administration électronique.

De plus, nous pensons que le développement de l'administration électronique forme un cadre optimal pour étudier toutes les questions relatives à ce principe. Plus concrètement, l'implantation de l'administration électronique suscite des phénomènes qui nous montrent combien la mise en application des principes classiques de protection des renseignements personnels devient ardue.

---

[173] Manuel FERNANDEZ SALMERON, *La protección de los datos personales en las administraciones públicas*, Madrid, Civitas , 2004, p. 39.

Ainsi, des changements majeurs à l'heure de mettre en relation les informations concernant les citoyens sont à l'origine de nouveaux risques. Voici l'idée exposée pour montrer cette problématique :

> « Avec l'apparition de techniques d'extraction de données et de rapprochements aléatoires qui permettent la mise en évidence de corrélations significatives, on atteint un niveau inédit dans la manipulation des données et on permet une construction massive des informations à l'insu des personnes. Si le regard se tourne de la formulation vers la circulation de l'information, le constat est identique. »[174]

Certains utilisent l'expression « explosion de l'information » pour parler de l'essor spectaculaire des moyens techniques permettant de collecter, traiter et transmettre l'information ainsi que de la forte expansion des sources d'information dans la plupart des sphères de l'activité humaine[175].

Bien sûr, nous pouvons imaginer la mise en place des techniques les plus modernes de gestion de l'information dans le contexte de l'administration électronique. Et cela notamment dans la perspective des flux d'information entre les différentes administrations.

Certains auteurs parlent des difficultés de réserver matériellement l'usage de l'information à une personne qui « tient tantôt à sa source, tantôt à la nature incorporelle de l'information »[176]. Est-on aujourd'hui face à l'impossibilité d'assurer l'utilisation « exclusive » des informations ? Pour montrer une telle circonstance, provoquée par la « volatilité » de l'information :

> « Objet évanescent, elle se prête difficilement à l'établissement d'un rapport d'exclusivité. Il en résulte une perte de maîtrise par la personne des circuits de l'information qui rendent les atteintes pratiquement indécelables en même temps qu'ils permettent des accès et utilisations furtives et abusives de tiers qui n'ont pas de titre à y prétendre. »[177]

---

[174] F. LESAULNIER, préc., note 57, p. 222.
[175] G.B.F. NIBLETT, préc., note 25, p. 9.
[176] F. LESAULNIER, préc., note 57, p. 222.
[177] *Id.*

Nous tenterons de montrer dans les pages qui suivent, comment des nouvelles pratiques, issues de l'avènement de l'administration électronique, illustrent cette problématique entourant, de façon particulière, l'application du principe de finalité reconnu dans les législations relatives à la protection des renseignements personnels. Pour cela, il était important d'identifier les limitations que l'application du principe de finalité rencontre dans le but de garantir de façon « réaliste » le respect du droit à la protection des renseignements personnels des citoyens dans le contexte de l'administration électronique.

## 3 Premières réflexions autour du nouveau modèle de circulation des informations

Nous allons devoir examiner dans le cadre de nos recherches les questions relatives à la finalité des traitements de renseignements personnels, ainsi qu'à la « réutilisation » des informations à des fins multiples.

Nous analyserons dans quelle mesure le phénomène de l'administration électronique change la donne, tout en laissant apparaître une crainte équivalente à celle qui existait par le passé, celle de l'interconnexion de l'ensemble des traitements publics en facilitant la centralisation des informations et donc des pouvoirs[178].

Il nous semble important de rappeler ici qu'il sera « de plus en plus difficile de circonscrire une fois pour toutes la finalité des traitements et que des systèmes réglementaires fondés sur des déclarations ou des autorisations *a priori* des finalités auront sans doute quelques difficultés à prendre en compte cette évolution permanente des finalités rendue possibles par les technologies modernes »[179].

Pour certains auteurs, « le fondement même de la réglementation des traitements informatiques traitant des données nominatives justifie que le principe de finalité puisse être apprécié différemment, étant donné les risques nouveaux suscités par les développements récents de la technologie »[180].

[178] Voir à ce propos : A.VITALIS, prec., note 21, p. 116.
[179] Y. POULLET ET T. LÉONARD, préc., note 30, p. 244.
[180] *Id.*, p. 246.

Nous sommes face à un changement de technologie, puisque la possibilité de partage des informations devient illimitée, mais également face à un changement de modèle d'État : l'État en réseau. L'administration électronique suppose ces deux changements majeurs, l'un purement technique et l'autre relevant plutôt du changement de paradigme depuis un gouvernement basé sur l'univers-papier vers un gouvernement électronique.

L'utilisation de nouveaux supports qui véhiculent des renseignements personnels et la facilité de transmission et de stockage de ceux-ci, nous oblige à nous demander si les dispositions existantes encadrent convenablement un tel scénario et prennent en considération l'éventuelle réutilisation des informations afin d'atteindre un niveau important d'efficacité administrative de la part de nos institutions.

La simplification des démarches et des formalités administratives par la mise en place d'un ensemble de téléprocédures peut modifier également le niveau d'exigence du citoyen envers l'administration. D'aucuns soulignent un changement majeur tirant son origine de certaines exigences propres au développement de ce nouveau modèle d'administration : « Les exigences de rapidité et de simplicité sur lesquelles repose le développement de l'administration électronique semblent commander une redéfinition du rôle de la hiérarchie, davantage invitée à coordonner les actions qu'à les contrôler »[181].

Les différents textes relatifs à la protection des renseignements personnels ne sont pas uniformes à l'heure de faire référence au principe de finalité et utilisent une multitude de termes qui rendent encore plus difficile l'établissement des contours d'un tel principe. Ainsi, nous pouvons observer que, dans les dispositions européennes et canadiennes faisant référence à l'idée préconisée par le principe de finalité, on utilise des expressions telles que « à une fin *non pertinente* à celle pour laquelle le renseignement a été recueilli ».

Dans certains textes, nous allons retrouver des termes de « finalité *différente* », tandis que dans d'autres dispositions, nous rencontrons « finalités *compatibles* »

[181] Lucie CLUZEL-MÉTAYER, *Le service public et l'exigence de qualité*, Paris, Dalloz, 2006, p. 275.

pour exprimer la même idée et pour imposer des obligations identiques. Ces termes peuvent-ils être jugés équivalents ?

Nous considérons que, dans le contexte de l'implantation des services du gouvernement électronique, cette question devient essentielle, ou même déterminante à l'heure de décider quels sont les traitements comportant des renseignements personnels qui vont être connectés afin que le citoyen puisse bénéficier d'une prestation électronique de services. Le rassemblement de certains traitements de renseignements personnels peut-il avoir pour résultat l'utilisation de ces informations à des finalités *compatibles, non différentes* ou *non pertinentes* par rapport aux finalités ayant motivé leur collecte ?

Cette question est essentielle au moment de déterminer ce que nous pouvons appeler les « familles de finalités » (qui doivent être mises en place pour pouvoir offrir chaque prestation électronique de services), puisque nous devons nous demander si ces familles ou grappes de finalités regroupent des traitements à finalités *compatibles*, *pertinentes* ou *différentes*. Comme nous pouvons l'observer, ces questions purement terminologiques présentent une certaine complexité à ne pas négliger dans le cadre de nos recherches.

Il est important d'analyser effectivement si « le service à l'usager » dont H. Maisl parle ou si « la nécessité d'un intérêt public important » peut justifier des finalités d'utilisation des renseignements personnels qui détermineront les modalités d'interconnexions qui doivent être mises en place dans le cadre de l'administration électronique.

*A priori*, une multitude d'enjeux gravitant autour de cette problématique méritent une réflexion plus approfondie dans le cadre de nos recherches. Qui va décider dans quelles circonstances certaines informations, qui dans le passé étaient séparées et cloisonnées à cause de la crainte de l'État *Big Brother*, vont être échangées par les différentes administrations au niveau national, provincial et même international ?

Il est essentiel de savoir si le citoyen aura son mot à dire dans cette réflexion, si les choix seront faits en collaboration avec le secteur public ou si le citoyen sera exclu

du processus de détermination des modalités d'échange des informations entre les organismes[182].

Comment le citoyen doit-il être averti des informations qui ont servi à la prise de décision le concernant par l'administration ? Pour qu'un vrai rapport de confiance entre le citoyen et l'administration puisse s'établir, il est essentiel que le citoyen connaisse, en conformité avec le principe de transparence, quelles sont les informations qui ont été prises en considération par les différents organismes dans l'adoption des décisions administratives.

Comment le principe de finalité va-t-il être conçu dans le futur, quand l'utilisation des renseignements personnels pour une seule fin ne pourra plus s'accorder avec une vision réaliste des prestations offertes au citoyen par l'administration ?

Il est également nécessaire d'analyser comment le principe de séparation informationnelle[183], dont certains auteurs parlent, peut s'accommoder du besoin de ressembler certaines informations dans le but d'offrir des prestations électroniques de services ou téléservices aux citoyens.

H. Maisl parle de la « Finalité des téléservices » et affirme :

> « Par rapport aux projets des années 70, un changement essentiel serait en cours si les projets de téléservices affichaient, comme finalité première, le service à l'usager ; le meilleur fonctionnement de l'administration et sa plus grande efficacité ne peuvent être que des finalités secondes pour les différentes applications sectorielles proposées. »[184]

Remarquons que H. Maisl parle de la finalité de chaque téléservice et non de la finalité de chaque traitement qui pourra être interconnecté dans le cadre de chaque téléservice, afin de répondre aux besoins de l'administration.

Voici un des plus grands enjeux de cette problématique : nous ne pouvons pas nier que parfois, les traitements de renseignements personnels peuvent avoir des

---

[182] FORUM DES DROITS SUR L'INTERNET, préc., note 163, p. 12. Ce rapport mentionne la « signature d'un contrat de vie privée entre le citoyen et l'État fixant les obligations et devoirs réciproques de chacun ». Il faut se demander si, concernant ce contrat, il s'agit d'un contrat d'adhésion ou si le citoyen va être en mesure de négocier avec l'État en cette matière.

[183] T. WÜRTENBERGER et G. SYDOW, préc., note 158, p. 364.

[184] H. MAISL, préc., note 157, p. 352.

finalités différentes de celle qui était à l'origine et avait motivé le traitement des renseignements personnels. La notion d'extension de finalité nous donnera les pistes pour comprendre de quelle manière cette situation est encadrée depuis quelques années et nous aurons l'occasion d'analyser si cette notion trouve son application effective dans le contexte de l'administration électronique. Nous pouvons dès lors envisager une « extension de finalité », qui devra être approuvée par l'autorité compétente à chaque fois et suite à des démarches très précises.

Nous pouvons encore imaginer la situation où son consentement serait demandé à la personne concernée à chaque fois que ses renseignements seraient utilisés pour une finalité autre que celle qui avait été déclarée au moment de la collecte.

À première vue, ces options peuvent nous sembler de bonnes solutions, mais le problème est beaucoup plus complexe, parce que ces options ne sont ni suffisantes ni réalistes pour un contexte comme celui qui est provoqué par la mise en place de l'administration électronique.

**4 - Une problématique présente dans différents contextes**

D'autres exemples illustrent cette problématique dans un contexte de circulation en réseau des informations où la question de la réutilisation des renseignements personnels entre en conflit avec le principe de finalité.

Pensons par exemple, les réseaux de chercheurs et de médecins qui fonctionnent grâce à des plateformes permettant l'échange électronique des données génétiques des sujets de recherche, afin de regrouper un nombre important d'informations, tout cela, dans un cadre régulateur des échanges, des accès et des règles relatives à la sécurité.

En examinant les enjeux entourant les échanges de données dans ces réseaux, nous constatons que le principe de finalité se trouve au centre de la problématique qui découle des réutilisations potentielles de ces informations, de l'indétermination de la notion d'utilisation secondaire, etc.

Nous pouvons reconnaître très clairement cette problématique si nous observons le cas des traitements relatifs aux renseignements personnels qui peuvent être contenus dans des documents à caractère public, ainsi que dans les cas où ces renseignements font partie d'un registre de nature publique[185]. L'utilisation d'Internet comme moyen de diffusion de ces documents et registres a fait naître un débat autour de la question relative à la finalité « unique » ou « multiple » de ces traitements contenant des renseignements personnels[186]. Il existe également l'idée selon laquelle, à l'heure actuelle, les informations ne représentent une richesse qu'à partir du moment où elles « circulent, s'échangent, se diffusent »[187].

Le phénomène de la diffusion libre sur Internet des informations contenues dans des registres publics et d'autres banques de données contenant des renseignements personnels à caractère public, nous montre qu'il est indispensable de trouver l'équilibre entre le droit à la vie privée et le droit à l'accès à l'information. Cette question illustre très clairement la problématique entourant l'interprétation du principe de finalité.

Ainsi, nous pouvons penser aux enjeux que représente la diffusion sur Internet de certaines informations qui, par le passé, étaient publiées exclusivement sur un support papier. Ce phénomène touche particulièrement certaines données à

---

[185] Voir : Michel GENTOT, « Administration électronique et protection de la vie privée : Renouveau de la problématique », dans George CHATILLON et Bertrand DU MARAIS (dir.), *L'administration électronique au service des citoyens*, Bruxelles, Bruylant, 2003, 325, p. 329. Cet auteur souligne qu'« un des exemples les plus manifestes, et sans doute des plus délicats, de ces changements que provoque la technologie, et qu'il convient de peser, est celui des données publiques lorsqu'elles deviennent accessibles sur Internet ».

Voir aussi à ce sujet : ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) et PRIVACY INTERNATIONAL (PI), *Privacy and Human Rights 2004, An International Survey of Privacy Laws an Developments*, 2004, p. 123.

Nous pouvons lire dans le rapport de 2004 ce qui suit :

*"Public records present some of the most difficult privacy challenges. On one hand, public records may assist individuals in ensuring that a government remains transparent and accountable. On the other, public records may be converted from this tool of citizen empowerment to one that empowers government and businesses to track citizens"*.

[186] Voir à ce sujet : P. TRUDEL, préc., note 148, p. 13.

P. Trudel dénonce une « rigidification » du principe de finalité, il écrit à la page 12 de ce texte que :

« Devant cette possibilité hypothétique d'abus, la solution retenue est d'imposer la mise en place de moyens technologiques pour assurer la protection des données personnelles contenues dans ces documents publics. Et cette protection est de limiter l'accès uniquement aux fins pour lesquelles un document est rendu public comme si ces fins étaient connues et spécifiées. Les décideurs vont devoir se mettre à spécifier les finalités du caractère public d'une information ».

[187] Frédéric LESAULNIER, préc., note 157, p. 218.

caractère public accessibles aux citoyens de façon libre et gratuite et qu'il est possible de trouver en un instant grâce aux puissants moteurs de recherche. Pensons par exemple à la diffusion sur Internet des décisions de justice, qui peuvent contenir des informations à caractère très sensible et un grand nombre de renseignements à caractère personnel[188].

La question de la finalité est au cœur du débat en Europe[189] et au Canada car, si ces informations sont diffusées, c'est pour répondre aux exigences de publicité et de transparence établies dans certaines lois, sans que cela se traduise par une utilisation de ces informations dans n'importe quel but[190].

---

[188] Voir à ce sujet : Rosario DUASO CALÉS, *La protection des données personnelles contenues dans les documents accessibles sur Internet : le cas des données judiciaires*, mémoire de maîtrise, Montréal, Faculté de droit, Université de Montréal, 2002, en ligne : https://papyrus.bib.umontreal.ca/jspui/bitstream/1866/2435/1/11449372.PDF (consulté le 11 janvier 2011).

[189] Rosario DUASO CALÉS, « Regulación europea sobre difusión de la jurisprudencia en Internet », dans Carlos GREGORIO et Sonia NAVARRO SOLANO (dir.), *Internet y sistema judicial en América Latina, Reglas de Heredia,* Buenos Aires, Ad-Hoc, 2004, p. 251 à 278.

[190] Jean-Claude SOYER, « L'avenir de la vie privée face aux effets pervers du progrès et de la vertu », dans Pierre TABATONI (dir.), *La protection de la vie privée dans la société de l'information*, T. 1, Paris, PUF, 2000, 7, p. 10.

Le problème tire son origine du changement des supports de données et des modes d'accès à l'information. Les questions relatives à la protection de la vie privée dans le contexte de la mise à disposition des documents publics sont nées avec l'utilisation des nouvelles technologies et du support numérique auxquels on recourt pour créer maints registres et documents. Sans doute, la mémorisation et le stockage en masse des données sont des phénomènes nouveaux, apparus grâce à l'utilisation des nouvelles technologies ; la nature de la diffusion des données publiques s'en trouve très souvent modifiée. Certains pensent qu'une donnée qui peut licitement devenir accessible dans un but particulier devrait bénéficier d'une protection qui tienne compte du fait que si elle est mise en mémoire et conservée pour un temps indéfini, la situation se complique. Les banques de données de jurisprudence nous fournissent un bon exemple de cette problématique. J.-C. Soyer renvoie à ce phénomène quand il dénonce les « effets pervers » du progrès auxquels les mécanismes de protection de la vie privée doivent faire face : « Comment cela ? Parce que l'informatique aux fabuleux bienfaits comporte, en revers, une aptitude effrayante : la mémoire totale, instantanée. À la fois par la minutie, l'immensité, la fréquence des informations recensées sur la vie quotidienne, donc largement privée : par une capacité sans limites de conservation de ces données, cela sous un volume de plus en plus restreint, qui permet le transfert instantané de telles informations ; par une aptitude de tri à la vitesse de la lumière, d'où s'ensuit la facilité des rapprochements et recoupements le plus inattendus, mais d'autant plus révélateurs ».

Deux aspects méritent notre attention. Premièrement la facilité du tri qui est rendu possible aujourd'hui grâce à la numérisation des documents ainsi que la recherche intégrale des documents par la multiplication des critères d'interrogation offerts. Pour certains, les critères d'accès à l'information peuvent changer la nature de la mise à disposition des documents et, ce qui est plus grave encore, l'usage qui sera fait de ces informations. Nous devons nous demander si ces informations peuvent servir à d'autres fins, tels que l'établissement de profils sur les citoyens, grâce au regroupement, par exemple, de ses renseignements de nature judiciaire, financière ou autres. Plusieurs questions se posent autour de ce phénomène : Quelle est la finalité de leur diffusion sur Internet et quels sont les usages licites de ces renseignements ? Où se trouve l'équilibre entre la

Quelles sont alors les « nouveautés » qui justifient l'examen de la question et qui, aux yeux de certains, exigent la révision des normes pouvant toucher aux modalités de publication de certaines données publiques afin de préserver le droit à la vie privée des personnes concernées ?

Pour ce qui est du consentement, mais dans une autre perspective, A. Lepage se pose la question, au moment d'appliquer la Loi I et L modifiée : « Qui ne voit la rigidité néfaste à laquelle aboutirait la nécessité absolue de s'en tenir au consentement de la personne pour procéder à des traitements ou à des transferts de données ? »[191].

Cette réflexion est évidemment d'actualité si nous pensons au contexte de l'administration électronique où des échanges et des transferts de données pourraient se produire afin de permettre la prestation aux citoyens de certains services.

De la même façon, nous devons tenir compte du fait que certains services que l'administration offre aux citoyens ne sont accessibles que si la personne a consenti à se dépouiller d'un certain nombre d'informations la concernant : « autant de données personnelles au traitement desquelles elle n'aura donc pu faire autrement que consentir »[192].

---

transparence et le respect à la vie privée dans le contexte de la diffusion généralisée des informations à caractère public qui sont détenues par l'administration ? À qui revient-il de déterminer la finalité particulière pour laquelle une information est mise à la disposition du public ? Comment arrive-t-on à déterminer cette finalité, à quels critères doit-on recourir ? Quelles sont les conséquences d'une détermination a priori ou bien a posteriori de cette finalité ? Pourquoi une finalité recevable dans le contexte de l'univers « papier » ne pourrait-elle pas être transposable aujourd'hui dans un environnement multimédia caractérisé par la numérisation des informations et leur circulation sur Internet.

Dans tous les cas, la notion de la finalité se trouve au cœur du débat entourant la circulation de ces renseignements à caractère personnel contenus dans des documents de nature publique. Nous pouvons imaginer les problèmes qui peuvent se poser à l'heure de limiter les utilisations que nous pouvons faire des informations de cette nature et aussi à l'heure de décider qui va devoir faire ces choix.

Voir également sur cette question : P. TRUDEL, préc., note 148, p. 12.

P. Trudel souligne l'idée suivante: « Devant cette possibilité hypothétique d'abus, la solution retenue est d'imposer la mise en place de moyens technologiques pour assurer la protection des données personnelles contenues dans ces documents publics. Et cette protection est de limiter l'accès uniquement aux fins pour lesquelles un document est rendu public comme si ces fins étaient connues et spécifiées. Les décideurs vont devoir se mettre à spécifier les finalités du caractère public d'une information ».

[191] A. LEPAGE, préc., note 69, p. 234.

[192] *Id*., p. 248.

Si nous pensons au modèle de « partage » des renseignements personnels, nous pouvons constater qu'il devient problématique d'opérer avec le consentement du sujet, surtout si nous imaginons ce consentement dans sa conception classique, qui est celle que nous connaissons aujourd'hui.

Si un citoyen doit donner son consentement à chaque fois que ses renseignements seront partagés entre deux organismes pour obtenir une prestation électronique de services, nous pouvons identifier plusieurs problèmes. Premièrement, si nous voulons instaurer un climat de confiance[193] entre l'administration et l'administré, le citoyen, qui doit donner son consentement à chaque fois qu'un organisme partage ses renseignements avec un autre organisme, peut se demander si ces organismes sont réellement dignes de confiance.

Pour certains, afin que la confiance puisse s'instaurer entre le citoyen et l'ensemble de l'appareil étatique « électronique », le citoyen ne devrait pas à chaque fois adresser son consentement à un organisme en particulier[194] et pour chaque interconnexion qui va devoir se faire dans le cadre des prestations électroniques de services. Il s'agit de réfléchir à des mécanismes plus adaptés à la circulation nécessaire des renseignements personnels, mais avec toutes les précautions et mesures capables d'assurer une protection des renseignements personnels à tout moment et pendant tout leur cycle de vie.

### 5- Secret et finalité

Certains auteurs se sont demandés si la finalité peut être un élément valable de la définition du « secret »[195] dans le contexte du secret des fichiers[196]. Ils ont vu que la

---

[193] Lire sur la question de la confiance dans le contexte du gouvernement électronique : Caroline J. TOLBERT et Karen MOSSBERGER, « The Effects of E-Government on Trust and Confidence in Government », 66 *Public Administration Review* (2006), vol. 66, n° 3, p. 354.

[194] Voir en ce sens : FORUM DES DROITS SUR L'INTERNET, *Recommandation sur le développement de l'administration électronique*, février 2003, p. 22, en ligne : http://www.foruminternet.org/recommandations/lire.phtml?id=493 (consulté le 14 avril 2010).
Le Forum des droits sur l'Internet signale que dans ce sens, « la réduction des contraintes imposées à l'usager permettrait également d'augmenter la confiance dans les rapports qu'il entretient avec l'administration ».

[195] Voir sur la notion de secret : René ALLADAYE, *Petite philosophie du secret*, Toulouse, Éditions Milan, 2006.

pratique du secret évolue constamment, en s'adaptant aux changements nécessaires de finalité, qui sont propres à un fichier « vivant ». Ainsi, la finalité connue au départ correspond exactement à la mission que poursuit le détenteur du fichier et « elle entraîne une certaine pratique du secret (…) les mesures de protection et les communications sont définies sur la base de cette finalité »[197].

Ainsi, ce serait une erreur de fonder toute la pratique du secret sur la finalité de départ, parce qu'il est irréaliste de croire que, lors de la création d'un fichier, toutes ses finalités peuvent être dégagées. Ces auteurs observent que les finalités sont nombreuses, mouvantes et que la finalité de départ est rapidement débordée par d'autres finalités, ce qui ne laisse comme seule opération à la rigueur envisageable que celle d'énumérer les finalités interdites. Ainsi, « ces changements en cours de gestion laissent penser qu'il est difficile de faire de la finalité un élément valable du secret »[198].

Ce lien établi entre finalité et secret nous semble tout à fait pertinent, notamment dans le contexte des fichiers du secteur public, puisqu'il est parfois question de savoir si certaines communications d'informations s'insèrent ou non dans la finalité première du fichier. Il semble encore plus approprié de privilégier cette vision « dynamique », qui s'adapte à la perfection au concept d'administration électronique.

Certains vont opposer d'une part les fichiers externes et d'autre part les fichiers internes, établis uniquement à l'usage interne de l'établissement et qui ne voient jamais leurs données transmises à l'extérieur.

Cette distinction, qui peut être transposable au scénario de l'administration, semble d'une grande fragilité pour certains experts qui considèrent qu'un fichier interne peut devenir très facilement externe. En conséquence, à cause du fait que le fichier peut évoluer pendant tout son cycle de vie en changeant ses finalités, et est donc, à

---

[196] Françoise GALLOEDEC GENUYS et Herbert MAISL, *Le secret des fichiers*, Paris, Éditions CUJAS, 1976, p. 259 et s.
[197] *Id.*, p. 259.
[198] *Id., p.* 260.

cause de ces transformations, « le fruit d'un jeu subtil de facteurs internes et externes », ce qui fait que « la pratique du secret, déterminée au départ, s'en trouve sérieusement modifiée »[199].

Certains parlent également d'un phénomène de « dilution du secret » lorsque l'on favorise les échanges d'informations sur les citoyens, parce que le Droit va fragiliser la protection de ces échanges, puisqu'il va accroître les risques de divulgations illégitimes : « à mesure que les textes multiplient les cas de justification légale du partage de l'information, ils étendent l'obligation de secret professionnel aux tiers autorisés à les connaître »[200].

Certains auteurs avancent trois processus qui entrent en jeu à l'heure d'examiner la question de la protection du « secret de la vie privée » : collecte, évaluation et transmission des données[201]. Le cycle de vie des informations et les différentes étapes ou processus dans le traitement de l'information peuvent effectivement être à l'origine d'une évolution dans les contours du secret. Cette vision plutôt dynamique sur la qualification ou la classification de l'information est capable d'appréhender d'une façon plus réaliste la circulation en réseau des informations.

[199] *Id., p.* 262.
[200] F. LESAULNIER, préc., note 57, p. 214.
[201] G.B.F. NIBLETT, préc., note 25, p. 18.

## CHAPITRE 2 GÉNÉALOGIE DES PRINCIPES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DU PRINCIPE DE FINALITÉ DANS LES INSTRUMENTS NORMATIFS EUROPÉENS ET CANADIENS

Les textes qui s'articulent autour des principes directeurs en matière de protection des renseignements personnels sont imprégnés de valeurs, qui ont dirigé les législateurs dans la rédaction des différentes dispositions. En effet, chaque principe de protection est le reflet d'un ensemble de valeurs voulant créer un dispositif respectueux des libertés et, plus particulièrement, du droit à la protection de la vie privée.

La volonté du législateur avait été de limiter la collecte, la communication et l'utilisation des renseignements personnels. Après examen de certains projets, tels que S.A.F.A.R.I. ou d'autres cherchant à interconnecter l'ensemble des bases de données publiques, l'objectif était de créer un code capable d'encadrer les traitements de renseignements personnels tout au long du cycle de vie des informations.

Ces principes se traduisent, d'une part, par l'établissement de certaines obligations pour les responsables des traitements et, d'autre part, par la reconnaissance des droits à exercer par les titulaires des renseignements personnels.

Quel a été l'objectif du législateur ? Qu'a-t-on recherché au moment de légiférer dans cette matière ? Que voulait-on protéger ? Les réponses à ces questions sont importantes pour comprendre quel modèle d'administration s'est mis en place, comme conséquence d'une vision de la protection des renseignements personnels qui s'est imposée grâce aux instruments normatifs en vigueur.
Le modèle de protection a influencé le modèle d'administration et les modes de gouvernance des traitements des renseignements personnels ont donné lieu à une structure de circulation des informations personnelles.

Cette structure s'est accordée à un mode de gouvernance des flux de renseignements personnels dans le but d'éviter une interconnexion généralisée des fichiers au sein de l'administration. Les premiers textes, tels que la Loi I et L en France ou la LPRP au Canada, ont visé le secteur public et c'est effectivement par rapport au secteur public que les risques ont été identifiés, l'administration étant, par ailleurs, la plus importante détentrice d'informations sur les citoyens. Les rapprochements entre les différentes bases des données sont les phénomènes à éviter par l'application des principes directeurs en la matière. Cet objectif est notamment envisageable à cause d'une structure d'État en silo, qui a rendu possible la répartition des renseignements par secteurs.

En étudiant l'historique de ces principes et, plus particulièrement, l'impact du projet S.A.F.A.R.I., nous observons que, au début, l'essentiel était d'établir quelques principes de base sur les questions de licéité des traitements.

La plupart des textes consacrent une première partie aux « Conditions générales de licéité des traitements de données à caractère personnel » (par exemple, au Chapitre II de la Directive 95/46/CE et Chapitre II de la Loi I et L modifiée).

Ainsi, les textes établissent plus concrètement certains « Principes relatifs à la qualité des données » (Section I et article 6 de la Directive 95/46/CE) et des « Principes relatifs à la légitimation des traitements des données » (par exemple, à la Section de la Directive 95/46/CE).
Les textes présentent fondamentalement des « Principes de base pour la protection des données », créant ainsi un catalogue de principes visant à encadrer les traitements de renseignements personnels (par exemple, au Chapitre II de la Convention 108). Ainsi, par exemple, dans le cas de la LPRPDE, ce code se trouve à l'Annexe 1 de la LPRPDE et énonce un ensemble de principes ayant pour but d'encadrer la protection des renseignements personnels pour le secteur privé.

En présentant des « Définitions et Principes » (par exemple, au Chapitre I$^{er}$ de la Loi I et L modifiée), les textes sont arrivés à définir certains termes essentiels et à délimiter le champ d'application des lois en matière de protection des renseignements personnels.

Nous procéderons premièrement à l'analyse de l'importance des principes directeurs aujourd'hui et de la manière dont leur nature joue un rôle important dans la recherche d'équilibre entre les différentes valeurs à harmoniser.
Par la suite, nous réaliserons une généalogie des principes en matière de protection des renseignements personnels. Pour cela, nous identifierons les textes qui feront l'objet de notre étude, afin de faire ressortir quelques particularités de ces instruments normatifs, articulés autour des principes.
Nous étudierons encore comment, pour atteindre l'objectif visant à empêcher l'interconnexion de toutes les bases de données publiques tout en privilégiant le cloisonnement des informations, les principes de la détermination des fins et de la spécification des finalités se trouvaient au centre du dispositif.
Ce principe de finalité fait partie « d'un tout » formé par un ensemble de principes que nous examinerons plus tard, afin de comprendre quel est le cadre de protection que le législateur européen et canadien a établi dans les textes en la matière.

## SECTION 1 Le rôle des principes dans le contexte actuel

Dans le nouveau modèle d'État en réseau, le droit à la protection des renseignements personnels entre en conflit avec d'autres droits et principes. Il faut noter que l'application du principe de finalité réclame une réflexion éthique à cause de l'équilibre qui doit être trouvé entre le droit à la protection de la vie privée et d'autres principes, tels que les principes d'efficacité, d'accessibilité, de qualité[202] et de rentabilité administrative[203].

Nous considérons qu'établir un équilibre entre ces principes est une tâche assez ardue cependant, à cause du caractère « relatif » de ces principes, nous pouvons envisager des solutions capables de protéger différentes valeurs, tout en se servant de ces principes en conflit pour réussir à établir des liens entre différents réseaux normatifs :

> « Des règles fixes contradictoires ne peuvent coexister. Les règles fixes sont tranchantes, exclusives. Elles jouent sur la séparation, sur la différence. Les principes directeurs sont eux relatifs. Des principes contradictoires peuvent subsister sans que l'un doive nécessairement prendre le pas sur l'autre. Les principes directeurs sont moins tranchants et grâce à cette qualité, ils sont capables d'établir des liens entre les normes et entre les réseaux normatifs. »[204]

Cette accentuation du rôle des principes, capables de créer des liens et rapports entre les différentes normativités, nous montre dans quelle mesure ils deviennent de plus en plus nécessaires. Il nous semble que, dans le contexte de l'administration électronique où des valeurs non nécessairement contradictoires mais pouvant entrer en conflit doivent coexister, les principes directeurs sont capables d'offrir une solution aux différents enjeux.

---

[202] Voir à ce sujet : Lucie CLUZEL-MÉTAYER, préc., note 181.

[203] Voir aussi au sujet de l'équilibre entre transparence et protection de la vie privée : *Éthique publique, Revue internationale d'éthique sociétale et gouvernementale*, « Les enjeux éthiques de la gestion de l'information », automne 2004, vol. 6, n° 2, Éditions Liber, Montréal, Québec, 2004.

[204] C.-A. MORAND, préc., note 19, p. 193 (nous soulignons).

Comme certains auteurs l'ont souligné, les principes sont appelés à encadrer des situations assez concrètes et spécifiques, même s'ils sont essentiellement généraux :

> « Seuls les principes, en raison de leur très grande généralité, sont capables de cadrer des activités qui doivent être appréciées dans leur spécificité. Les règles fixes, à l'instar des cartes trop détaillées, s'épuiseraient dans cette tâche »[205].

Pour certains, le principe et la règle juridique ont tous les deux un lien avec l'ordre juridique positif, sauf que, même si les deux notions ont beaucoup en commun, « il existe entre elles une différence de nature et une inégalité d'importance dans l'ordonnement juridique qui n'est pas sans conséquence sur leur rôle et sur leur interprétation »[206]. Ainsi, la règle est édictée en vue d'une situation juridique déterminée et apparaît souvent comme une application des principes ou des exceptions.

Au contraire, le principe comporte une série indéfinie d'applications, préside à un certain nombre de règles et supporte des règles dérogatoires[207]. En effet, c'est grâce aux principes que la situation particulière est analysée et qu'en procédant à un examen « au cas par cas » on parvient à établir les règles encadrant chaque traitement, chaque rapprochement de données ou chaque transmission à des tiers.

Comme certains experts l'ont souligné, les principes participent à la construction d'un système de protection des données personnelles à la recherche d'un équilibre entre des intérêts et des libertés qui s'opposent, lui seul pouvant offrir « une réponse adéquate à une évolution technologique en pleine ébullition »[208].

Certains auteurs expliquent que dans un tel contexte, se modifiant constamment à cause des évolutions technologiques, les principes deviennent essentiels :

> « Il nous semble en effet qu'à l'éclatement et à la spécialisation, dans un environnement technologique voué à changer toujours, il paraît sage de répondre par une quête de l'ordre et de l'équilibre, aussi

[205] *Id.*, p. 192.
[206] F. LESAULNIER, préc., note 57, p. 23.
[207] Voir sur ces questions : *Id.*, p. 23 et 24.
[208] Y. POULLET et T. LÉONARD, préc., note 30, p. 231.

> fragiles soient-ils, un équilibre qui ne peut passer que par la recherche non de dogmes, mais de directives propres à servir de guide sans grand risque d'erreur. Et surtout, si les principes ainsi dégagés sont relatifs, la finalité, les valeurs qui les inspirent, et n'ont rien d'indécis. »[209]

Ces principes pouvant paraître flous, indéterminés et même « relatifs », renferment des valeurs « absolues », très concrètes et facilement reconnaissables. C'est facilement visible dans le contexte de la protection des renseignements personnels, où les valeurs inspirant les principes directeurs en la matière sont ceux présents dans les différents instruments normatifs.

La structure *en réseau* du droit qui va encadrer nos recherches, pourra également établir des équilibres entre divers intérêts consacrés par les principes directeurs reconnus dans des ordres juridiques différents :

> « La structuration en réseaux comporte une part importante d'organisation. Le droit peut établir des hiérarchies souples avec les principes émanant d'un ordre juridique supérieur ou entre les divers intérêts consacrés par les principes directeurs faisant partie d'un ordre juridique donné. »[210]

Nous devons signaler que certains textes portant sur l'Administration publique ont pour objectif pour les prochaines années une utilisation optimale des possibilités des nouvelles technologies par les différents ministères et organismes et proposent de favoriser leur concertation et le partage de leurs ressources[211]. Il faut noter que le principe d'efficacité de l'administration publique est présent dans la plupart des lois en la matière. Pour cette raison, il est primordial de comprendre comment ces objectifs vont jouer dans la mise en place du nouveau modèle d'administration, tout en respectant les grands principes de protection des données personnelles.

Bien sûr, les principes de loyauté, et très spécialement celui de proportionnalité, vont devoir également guider les conditions de création de chaque traitement

---

[209] F. LESAULNIER, préc., note 57, p. 23 (nous soulignons).
[210] C.-A. MORAND, préc., note 19, p. 206.
[211] *Loi sur l'administration publique*, L.R.Q., c.A-6.01.

automatisé de renseignements personnels, ainsi que la mise en place des interconnexions. Dès lors, ces principes seront essentiels à l'heure d'analyser les fondements du principe de finalité, étude que nous entamerons dans le cadre de nos recherches. Pour certains experts, quelques principes, comme celui de la finalité et celui de proportionnalité, sont « de nature à prévenir les abus liés au très faible coût et à la simplicité d'engranger, de réutiliser, de copier l'information numérisée »[212].

Nous observons que le principe de proportionnalité joue un rôle majeur dans l'établissement de certains équilibres, comme cela a été souligné : « la règle par laquelle le législateur fait prévaloir l'intérêt général sur la liberté de l'individu doit satisfaire à une double exigence : être claire et précise (…) et satisfaire au principe de proportionnalité, lequel a rang de principe constitutionnel »[213]. Il faut noter que le tribunal constitutionnel allemand a rappelé que le besoin d'information des autorités publiques ne peut prévaloir sur le droit individuel à la maîtrise des données personnelles que si le principe de proportionnalité est dûment respecté[214].

Le principe de proportionnalité, corollaire du principe de finalité, a toujours été pris en considération par la CNIL, qui a « toujours eu à cœur de vérifier le respect de cette proportionnalité entre les moyens technologiques mis en œuvre et la finalité poursuivie par un traitement, sans oublier la stricte délimitation des destinataires des informations collectées »[215]. Ainsi, l'exercice de vérification, devant confirmer l'absence de solutions techniques alternatives pour atteindre une certaine finalité, permet de confirmer par la justification de la proportionnalité le traitement en question.

Il faut noter également que c'est en application de la règle de la proportionnalité que la CNIL a défini un « principe de sectorisation » selon lequel une large diffusion, tous secteurs confondus, de certaines informations constituerait une

---

[212] Marie GEORGES, « Protéger les données à l'heure des réseaux », *Liberté, Risque et Responsabilité*. Nouveaux repères à l'heure de la mondialisation et du terrorisme international, CAHIERS DE L'IFRI, Paris, La Documentation française, 2002, p. 1116.
[213] G. GÉRIN, préc., note 62, p. 114.
[214] Voir à ce sujet : *Id.*, p. 122.
[215] N. MALLET-POUJOL préc., note 50, p. 7.

atteinte disproportionnée à la vie privée, et cela en raison du risque de détournement de finalité[216].

Quelques-uns, à l'heure d'examiner et d'évaluer certains traitements, préconisent l'application du principe de précaution, qui va imposer pour chaque cas « une certaine retenue »[217]. Prenons l'exemple de la biométrie afin de comprendre comment le choix d'une fonction de vérification ou d'identification va dépendre fondamentalement de la finalité du système biométrique en question et des circonstances dans lesquelles il sera mis en place.

Il est dès lors essentiel que l'instrument en question puisse servir la finalité pour laquelle les données ont été collectées et ne pas être « inutilement surdimensionné ». Ce qui doit être évité à tout prix, c'est que l'instrument en question ne soit disproportionné par rapport à la finalité première qu'il doit remplir. Si nous continuons avec cet exemple, puisqu'il n'y a pas de liste exhaustive des finalités légitimes, dès que les finalités sont déterminées, le système technique ne doit permettre ni la collecte, ni le traitement de plus de données personnelles que les finalités n'en exigent[218].

Nous aurons l'occasion d'approfondir le rôle que peut jouer la règle de proportionnalité dans l'exercice relatif à la pondération des intérêts pour arriver à appliquer le principe de finalité.

Comme plusieurs auteurs l'expliquent : « la recherche de la proportionnalité échappe à toute réglementation préalable ; elle se fait dans chaque cas d'espèce, ce qui n'est pas incompatible avec la construction progressive d'une doctrine, sous le regard vigilant du juge »[219].

---

[216] Christiane FÉRAL-SCHUHL, *Cyber droit, Le droit à l'épreuve de l'Internet*, Paris, Dalloz, 2006, p. 12 et 13.

[217] COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL, CONSEIL DE L'EUROPE, *Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques*, février 2005, p. 2 et s.

[218] *Id.*

Il faut souligner que les données biométriques ont une particularité, puisqu'elles contiennent souvent plus d'informations que celles étant nécessaires à la vérification ou à l'identification des personnes. Normalement, pour les données non biométriques, l'exercice est moins problématique.

[219] L. CADOUX, préc., note 60, p. 14.

Pour ce qui est de la protection des renseignements personnels, le principe de proportionnalité est utilisé par les autorités de contrôle au cas par cas, ce qui donne effectivement une doctrine qui nous aide à comprendre l'étendue d'un tel principe, ainsi que de celui faisant référence à la finalité.

La CNIL, dans son 24 Rapport d'activité[220], a mis l'accent « sur quatre principes qui sont largement pris en compte par le programme gouvernemental de développement de l'administration électronique en France : le principe de finalité, le principe de transparence, le principe de sécurité graduée et le principe de pluralité des identifiants ».
Elle insiste sur le principe de proportionnalité, afin de « simplifier sans multiplier les interconnexions », et parle en outre de la finalité de chaque interconnexion :

> « (…) le respect du principe de proportionnalité justifie que tout projet de mise en relation de fichiers fasse l'objet d'une vigilance particulière et d'un contrôle spécifique de la CNIL, portant en particulier sur l'appréciation de la finalité même de l'interconnexion (nécessité d'un intérêt public important), sur la pertinence des données échangées, les destinataires habilités à connaître des données, l'information claire et explicite des personnes concernées par ces échanges. En outre, si les informations susceptibles d'être rapprochées sont protégées par un secret professionnel, les échanges de données ne peuvent être que si, au préalable, une disposition législative spécifique est intervenue pour lever celui-ci. »[221]

Certains auteurs nous rappellent qu'effectivement, les normes en matière de gouvernement en ligne sont fréquemment exprimées sous la forme de principes directeurs, une tendance s'observant souvent dans le domaine des technologies de l'information[222].

---

[220] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *24 Rapport d'activité*, 2003, p. 77, en ligne: http://www.cnil.fr (consulté le 11 février 2010).
[221] *Id*., p. *78*.
[222] Pierre TRUDEL, « État de droit et e-gouvernement », dans Karim BENYEKHLEF et Pierre TRUDEL (dir.), *État de droit et virtualité*, Montréal, Éditions Thémis, 2009, 373, p. 387.

**1- Les textes articulés autour des principes**

Nous avons dû faire un choix quant aux textes qui feront l'objet de nos travaux afin de limiter, d'une certaine façon, l'analyse de ces principes repris dans tous les instruments légaux en la matière.

Nous procéderons d'abord à l'étude de la Directive européenne de 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, texte qui a été à l'origine de toutes les lois européennes en la matière. Plus tard, nous examinerons la manière dont la Convention, du 28 janvier 1981, le Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[223] et certains textes européens, notamment la Loi I et L modifiée, s'articulent à partir des principes directeurs.

Par la suite, nous analyserons comment les textes canadiens reprennent les principes essentiels en matière de protection des données personnelles, pour finalement étudier comment l'esprit du principe de finalité a été repris par le législateur fédéral canadien.

Si nous observons la législation canadienne et européenne, nous pouvons citer parmi ces principes : le principe de finalité, de qualité des données, de proportionnalité, de loyauté, de transparence, de l'information des personnes concernées et de sécurité.

Mais nous devons citer également les principes faisant notamment référence au droit d'accès, de rectification, d'opposition et le principe du consentement de la personne concernée.

Bien sûr, pour les fins de notre recherche, c'est le principe de finalité et par conséquent celui faisant référence à la spécification des finalités qui sont au centre de nos intérêts. Cependant, il est important de faire un rapide survol des autres

[223] *Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel du 28 janvier 1981 du Conseil de l'Europe*, S.T.E. nº 108 (ci-après Convention 108).

principes puisque, et nous le verrons plus tard, certains parmi eux doivent être appréhendés à l'aide du reste des principes.

### A- Le contexte européen

Il est primordial de comprendre le rôle majeur que l'Union européenne a joué dans l'établissement d'un cadre légal pour protéger les renseignements personnels à niveau mondial. Voici l'idée que A. L. Newman avance à ce sujet : « *Europe, long viewed as the little brother of international economic governance, has transformed the global privacy debate by pressing for high levels of protection, especially in the private sector* »[224].

Cet auteur identifie trois étapes, reliées entre elles, dans l'importante démarche européenne en la matière, à savoir : une première étape qui est celle des premières législations en matière de protection des renseignements personnels dans les années 1970 ; une deuxième déterminée par l'adoption, dans les années 1990, de la première Directive européenne en la matière; et finalement, une troisième étape caractérisée en grande partie par la promotion des régulations fortes en matière de protection des renseignements personnels à niveau mondial[225].

A. L. Newman n'hésite pas à affirmer que, si nous observons comment la question de la protection des renseignements personnels est devenue un des domaines les plus importants en matière de gouvernance de la société de l'information, l'action de l'Europe dans cette matière a transformé le débat. L'exemple de la question de la régulation de la protection des renseignements personnels nous permet d'observer que l'Europe occupe une place de plus en plus importante dans la gouvernance globale.

En effet, si l'Europe a été à l'origine des plus importantes régulations en matière de protection des renseignements personnels, nous reconnaissons également une nette volonté de créer des règles globales, faisant parfois même face à la claire opposition d'autres gouvernements :

---

[224] A. L. NEWMAN, préc., note 116, p. 3.
[225] *Id.*, p. 6.

> *« Despite intense opposition from the United States and other major governments, Europe not only has developed an alternative to the* laissez faire *mentality concerning personal information but is leading the race to set global privacy rules. This outcome is quite striking given fears that national regulatory protections would fall victim of the pressures of the international economy. It is even more surprising given the general dominance of U.S. regulatory preferences in most other governance concerns of the digital economy, ranging from intellectual property to Internet domain names.* »[226]

Le système basé sur ces principes en matière de protection des renseignements personnels a été à l'origine d'une telle démarche et incarne à la perfection un modèle qui a été transposé vers d'autres pays, comme nous aurons l'opportunité de le mentionner dans les pages qui suivent.

Le système est devenu *de facto* un modèle au niveau international, ce qui fait que, quand l'Europe adopte une position en matière de régulation ayant des conséquences à niveau extraterritorial, les autres pays se voient obligés de faire des choix en ce qui concerne la réforme de leurs propres lois nationales.

Si nous regardons le droit européen, nous observons que la Directive 95/46/CE établit que « les principes de la protection des droits et des libertés des personnes notamment du droit à la vie privée, contenus dans la présente directive précisent et amplifient ceux qui sont contenus dans la Convention, du 28 janvier 1981, du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel »[227].

En effet, les principes se retrouvant à la Convention 108 et à la Directive 95/46/CE s'appliquent dans les mêmes conditions au secteur public et au secteur privé.

Il faut noter également que la Directive 95/46/CE souligne que les principes de protection des renseignements personnels se trouvant dans ce texte doivent trouver ainsi leur expression :

> « (…) d'une part, <u>dans les obligations mises à charge des personnes, autorités publiques, entreprises, agences ou autres organismes</u> qui traitent des données, ces obligations concernant en particulier la

[226] *Id.*, p. 3.
[227] Considérant n. 11 de la Directive 95/46/CE.

> qualité des données, la sécurité technique, la notification à l'autorité de contrôle, les circonstances dans lesquelles le traitement peut être effectué, et, d'autre part, dans les droits donnés aux personnes dont les données font l'objet d'un traitement d'être informés sur celui-ci, de pouvoir accéder aux données, de pouvoir demander leur rectification, voir de s'opposer au traitement dans certaines circonstances. »[228]

Ces principes doivent se traduire par l'établissement de certaines obligations pour les responsables des traitements, mais aussi par la reconnaissance des droits des personnes concernées par le traitement des renseignements personnels.

D'aucuns ont fait savoir que même si les règles que la Directive 95/46/CE établit sont plus explicites et plus développées que celles se trouvant dans la Loi Informatique et Libertés de 1978, elles font toutes parties du même ordre d'idées[229].

Ces principes doivent être transposés dans les dispositions législatives de chaque État membre afin de créer un régime de protection équivalent au sein de l'ensemble de l'Union Européenne. Dans l'état actuel, l'ensemble des pays européens ont un régime homogène en la matière, ce qui donne comme résultat une protection équivalente des données personnelles dans tous les États membres.

Nous assistons depuis un certain temps à un mouvement visant à démontrer le besoin d'adapter la Directive 95/46/CE aux technologies du 21e siècle et nous notons qu'un certain nombre de travaux sont aujourd'hui présentés afin de témoigner du besoin d'adaptation de ce texte européen à une nouvelle réalité.

Ainsi, l'autorité de protection britannique, le *Information Commissioner's Office*, ICO, a lancé une étude visant à ouvrir la voie pour réformer la Directive 95/46/CE, étude dans laquelle nous pouvons analyser la manière dont les auteurs identifient les points forts et les points faibles de cet instrument européen[230].

L'articulation du texte communautaire, réalisée autour de l'ensemble des principes de protection, a été identifiée en mai 2009 comme étant un des points forts de la Directive 95/46/CE.

---

[228] Considérant n. 25 de la Directive 95/46/CE (nous soulignons).
[229] G. BRAIBANT, préc., note 56, p. 35.
[230] Neil ROBINSON, Hans GRAUX, Maarten BOTTERMAN et Lorenzo VALERI, *Review of the European Data Protection Directive*, Sponsored by the Information Commissioner's Office, RAND Corporation, 2009.

Pour les auteurs du rapport, le fait d'avoir un encadrement basé sur des principes apporte sans aucun doute à la Directive 95/46/CE une certaine flexibilité, étant donné que ce texte reprend des principes sans aller dans les détails pour des secteurs spécifiques. On avance d'ailleurs à propos de cette flexibilité, qui tire son origine de l'articulation basée dans cet ensemble de principes :

> « *Many of the Directive's obligations remain relatively high level. The framework approach based on principles allows Member States to implement the necessary measures while taking into account local traditions and sensitivities, and the needs of specific sectors.* »[231]

Comme nous avons pu le constater dans les lignes précédentes, la Directive 95/46/CE concrétise les principes que la Convention 108 avait déjà instaurés au début des années 1980. Le Préambule de la Convention 108 soulignait l'idée suivante : « Il est souhaitable d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés »[232].

Certains soulignent à ce propos que « les principes contenus dans la Convention 108 doivent s'entendre comme étant le plus petit dénominateur commun existant entre les pays membres »[233].

La Convention 108, qui est ouverte à l'adhésion de pays non membres, a été très fortement inspirée de la Loi I et L, particulièrement dans sa façon d'articuler le texte grâce à des principes généraux créant la base de protection minimale des renseignements personnels faisant l'objet d'un traitement.

Bien sûr, la Loi I et L avait déjà établi en 1978 des principes équivalents, qui étaient au cœur de la législation française et qui ont très fortement inspiré la Convention 108 et, par conséquent, la Directive 95/46/CE. La CNIL note à ce

---

[231] *Id.*, p. 24.
[232] Préambule de la Convention 108.
[233] Cynthia CHASSIGNEUX, *Vie privée et commerce électronique*, Thémis, Montréal, 2004, p. 118.

propos, juste avant l'adoption de la Loi I et L modifiée[234] : « Ce dispositif, reposant sur l'énoncé de principes généraux et sur la confiance à l'égard d'une autorité indépendante, doit être préservé afin que la loi nouvelle puisse conserver une souplesse suffisante qui seule assurera sa permanence »[235].
En effet, l'arrivée de phénomènes tels que l'internationalisation des échanges ne doit pas provoquer la relativisation de la portée des principes et garanties reconnus en France depuis des années ou faire douter de leur pertinence. Par contre, elle doit « impérativement inciter à les voir confirmés et élargis par la loi nouvelle, comme d'ailleurs la directive européenne l'a fait en consacrant sur de nombreux points l'expérience française »[236].

Dans le cadre de nos travaux, nous tracerons l'historique du principe de finalité. En conséquence, la Loi I et L sera étudiée afin de comprendre quel a été le chemin parcouru avant même l'adoption de cette loi, en 1978, jusqu'à aujourd'hui dans la définition d'un tel principe. Cependant, nos travaux porteront particulièrement sur la Loi I et L modifiée, texte qui est actuellement en vigueur en France et qui est le résultant de la transposition de la Directive 95/46/CE en droit français, par l'adoption de ce nouveau texte en 2004.

C'est en 1998 que le Rapport « Données personnelles et société de l'information »[237], établit une division entre deux types de principes à caractère fondamental que nous retrouvons dans la Directive 95/46/CE : « Ainsi apparaissent les principes fondamentaux, généraux (proportionnalité, sécurité, transparence) ou propres à la matière (finalité, confidentialité), dont la mise en œuvre doit être inscrite dans les lois et règlements de chaque pays et peut être précisée par des codes de conduite sectoriels. »[238] Nous constatons alors que ce principe de finalité se présente comme un principe en matière de protection des renseignements

[234] *Loi 78-17 du 6 janvier 1978 modifiée* (ci-après : Loi I et L modifiée).
[235] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Avis sur le Projet de Loi modifiant la Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, 26 septembre 2000, p. 3.
[236] *Id.*, p. 2.
[237] G. BRAIBANT, préc., note 56.
[238] *Id.*, p. 35 (nous soulignons).

personnels, tel que celui de confidentialité, tous les deux visant à accorder une protection spécifique et renforcée.

Et c'est en comparant la Loi I et L de 1978 avec la Directive 95/46/CE que nous vérifions que l'une et l'autre se fondent sur un corpus de principes communs que, comme l'auteur de ce Rapport l'a souligné, « l'on retrouve d'ailleurs dans de nombreuses législations nationales et dans des textes internationaux, comme ceux du Conseil de l'Europe, de l'O.C.D.E. ou des Nations Unies ».[239]

En effet, ces principes communs, qui concernent les données, mais également les traitements et les personnes[240], sont à la base de toutes les législations en matière de protection de renseignements personnels.

Il faut noter qu'à différence du moment précédant la transposition, dans la Loi I et L modifiée, nous remarquons que « la distinction entre les secteurs public et privé n'est plus de mise actuellement, le secteur privé cherchant lui aussi à connaître les moindres faits et gestes des internautes. Big Brother n'est plus seulement personnalisé par l'État (…) »[241]. En effet, la Loi I et L modifiée se rapproche du texte de la Directive 95/46/CE en établissant que les traitements des secteurs public et privé seront soumis aux mêmes conditions.

Comme le mentionne la CNIL, l'extension de l'informatique et des nouvelles technologies à la sphère marchande justifie qu'il soit finalement soumis au double régime qui caractérisait la Loi I et L, et qui supposait l'examen préalable des traitements publics et la simple déclaration des traitements privés[242].

Mais cela, ne peut causer l'abaissement du niveau des garanties dans la mise en œuvre, par le secteur public, de certains fichiers ou traitements de données particulièrement sensibles, tels que les interconnexions des fichiers, « à l'égard desquels la loi du 6 janvier 1978 a prévu dans le souci d'apaiser les craintes qu'ils

[239] *Id.*, p. 36.
[240] Voir sur ce sujet : *Id.*, p. 36.
[241] C. CHASSIGNEUX, préc., note 233, p. 128 et 129.
[242] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 235, p. 1.

pouvaient légitimement susciter, des mécanismes de contrôle rigoureux »[243]. Nous aurons l'occasion d'étudier dans les pages qui suivent les particularités du régime spécifique que le législateur français a voulu accorder au phénomène des interconnexions entre fichiers publics.

Le législateur a mis fin en 2004 à une dichotomie entre les fichiers du secteur public et ceux du secteur privé, dichotomie fondée sur le critère organique du statut public ou privé du responsable du traitement et qui, pour certains, est une *summa divisio* « désormais désuète »[244].

### B- Le contexte canadien

Nous avons étudié dans les pages précédentes la façon dont le système Informatique et Libertés en France et le cadre européen de protection des renseignements personnels ont vu le jour afin de répondre aux risques informationnels. Le Canada occupe une place importante dans le mouvement de la protection des renseignements personnels au niveau mondial, et cela à cause de ses particularités uniques en Amérique du Nord.

Même si le droit américain en matière de protection des renseignements personnels ne fera pas l'objet d'une étude dans le cadre de nos travaux, il est important de comprendre comment se réalise l'encadrement de la *privacy* aux États-Unis pour mieux saisir la stratégie canadienne en la matière.

En effet, si nous regardons comment le droit à la protection de la vie privée est conçu aux États-Unis et en Europe, nous pouvons repérer d'énormes différences. Plus précisément, comme certains auteurs[245] l'ont très bien souligné, nous pouvons observer une très claire distinction entre le droit américain et le droit européen en matière de vie privée. Si le droit à la *privacy* aux États-Unis est basé sur un système

---

[243] *Id.*, p. 2.

[244] Anne SENDRA, « Informatique et Libertés : que change la réforme du 6 août 2004? », dans *Le harcèlement numérique*, Jean-Luc GIROT (dir.), Paris, Dalloz, 2005, 187, p. 190.

[245] Voir: Avner LEVIN, Mary Jo NICHOLSON, « Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground », 2:2 UOLTJ, 357 (2005), 391.
James Q. WITHMAN, « The two western Cultures of Privacy: Dignity versus Liberty », 113 Yale L.J. 1151 (2004), 1163.

qui repose sur la valeur de la « liberté », le droit européen sur la vie privée gravite autour de la notion de « dignité humaine ».
Pour ce qui est du contexte américain, le droit à la vie privée peut donc être considéré comme un aspect de la liberté, tandis que, dans le contexte européen, la vie privée est conçue comme un aspect de la dignité.

De plus, les attaques pouvant limiter le droit à la vie privée dans les deux systèmes trouvent leur origine différemment : « *On the one hand, a European interest in personal dignity, threatened primarily by the mess media; on the other hand, an American interest in liberty, threatened primarily by the government* »[246].
Selon J.Q. Whitman, la résistance aux États-Unis à la *privacy* de Warren et Brandeis[247] a toujours été fondée en deux valeurs : la liberté de presse et le libre marché[248].

Si les Européens et les Américains perçoivent le droit à la protection de la vie privée de façon très différente, où se place le Canada par rapport à ces deux traditions juridiques ?
A. Levin et M.J. Nicholson affirment : « *We believe that Canada is well positioned to become a bridge between Europe and the US* »[249].
Et cela, parce qu'ils considèrent qu'une autre perception du droit à la vie privée venant du Canada est possible : « *We believe an alternative foundation is possible, based on the idea of autonomy and personal control as is emphasized in Canada* »[250].

A. Levin et M.J. Nicholson remarquent que le droit à la protection de la vie privée au Canada n'est pas uniquement basé sur la dignité humaine ou sur la liberté, mais

[246] J. Q. WITHMAN, préc., note 245, 1219.
[247] S.D. WARREN, L.D. BRANDEIS, « *The Right to Privacy* », 4 Harv. L.Rev. 193 (1890). L'auteur fait référence à cet article paru en 1890 qui, pour une grande partie de la doctrine, suppose le travail scientifique ayant contribué de façon définitive à la consécration du droit à la protection de la vie privée aux États-Unis.
[248] J. Q. WITHMAN, préc., note 245, 1208.
[249] A. LEVIN, M. J. NICHOLSON, préc., note 245, 393.
[250] *Id.*, 394 (nous soulignons).

également, et surtout, sur des concepts pouvant nous faire penser à la notion d'autodétermination informationnelle. Ils expliquent :

> « *We believe Canadians are concerned as to the manner in which their personal information is handled once it is out of their hands, not only because this represents a threat to their liberty if it is mishandled by the public sector, or a threat to their dignity if it is mishandled by the private sector, but also because Canadians do not want to lose their autonomy, their control over this information, which is, after all, personal.* »[251]

Il nous semble que cette vision correspond effectivement à l'idée qui a inspiré les textes canadiens en la matière et qui a posé le Canada en Amérique du Nord et dans le monde comme un pays respectueux du droit à la protection de la vie privée.

Les textes accordant une protection aux renseignements personnels s'articulent autour de certains principes qui établissent un cadre général de protection. Nous retrouvons dans les instruments légaux, d'un côté et de l'autre de l'Atlantique, des obligations à respecter afin d'être en conformité avec toute une série de principes que les premiers textes dans la matière ont déjà adoptés et qui sont à la base des législations actuelles.
Les principes se retrouvant dans les textes internationaux sont également présents dans les lois nationales, ce qui témoigne d'une certaine homogénéité en la matière.

Les principes se trouvant dans les textes européens se trouvent donc également dans les textes canadiens au niveau fédéral, ce qui sans doute a motivé en 2001 que le Groupe de travail de l'article 29 sur la protection des données à caractère

[251] *Id*.

personnel[252] produise un avis[253] sur le niveau de protection garanti par la Loi sur la protection des renseignements personnels et les documents électroniques[254].

Par la suite, la Commission européenne a accordé le « niveau de protection adéquat » des données à caractère personnel assuré par la LPRPDE[255], grâce notamment à la présence dans ce texte canadien des principes basiques de protection que la Directive 95/46/CE établit.

La LPRPDE constitue la législation canadienne s'appliquant exclusivement au secteur privé[256] dans le cadre des activités commerciales et non au secteur public, encadrement naturel pour le développement du gouvernement électronique.

Dans les dispositions contenues dans la LPRP, qui a pour but d'encadrer la protection des renseignements personnels dans le secteur public fédéral, nous retrouvons également l'ensemble des principes de protection, même si de façon plus limitée.

Sur le plan canadien, la LPRPDE a reçu la sanction royale le 13 avril 2000, elle s'applique aux organisations du secteur privé qui collectent, utilisent ou communiquent des données personnelles dans le cadre d'activités commerciales et elle est rentrée en vigueur en trois étapes.

---

[252] Ci-après : Le Groupe de l'article 29.

[253] GROUPE « ARTICLE 29 » SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES, *Avis 2/2001 sur le niveau de protection garanti par la Loi canadienne sur la protection des renseignements personnels et les documents électroniques*, 2001.

[254] *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5. (ci-après : LPRPDE).
Notons que le Canada a une loi encadrant la protection des renseignements personnels dans le secteur public depuis 1985 : *Loi sur la protection des renseignements personnels*, L.R.C. 1985, c. P-21. (ci-après : LPRP).

[255] COMMISSION EUROPÉENNE, *Décision de la Commission du 20 décembre 2001 constatant, conformément à la Directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, (JO L 2 du 4.1.2002, p. 13–16).*

[256] Voir sur cette adéquation de la législation canadienne relative au secteur privé: Rosario DUASO CALÉS, « El derecho a la protección de los datos personales en el ámbito privado en la legislación federal canadiense y quebequense », dans Esther MITJANS et José Maria CASTELLA (dir.), *Derechos y Libertades en Canadá*, Barcelona, Ed. Atelier, Col. Canadiana, 2005, de p. 355 à 371.

Comme la Commission Européenne l'a notifié en 2001, « la loi canadienne (LPRPDE) énonce l'ensemble des principes de base nécessaires à un niveau de protection adéquat pour les personnes physiques, même si elle prévoit des exceptions et des restrictions en vue de protéger des intérêts publics majeurs et de reconnaître certaines informations qui existent dans le domaine public »[257].
En effet, la LPRPDE est venue compléter l'encadrement législatif canadien grâce à l'étendue de ces principes de protection dans le secteur privé. Comme certains l'ont déclaré :

> « En couvrant seulement le secteur public, la protection accordée aux renseignements personnels ne correspondait pas aux exigences de l'article 25 de la Directive 95/46/CE. En effet, cette Directive entend protéger l'ensemble des données personnelles quel que soit le secteur d'activité de l'organisme collectant lesdites données. De plus, dans une optique internationale, cette directive vise à garantir l'intégrité des informations susceptibles de faire l'objet d'un transfert au-delà des frontières nationales des États membres de l'Union. »[258]

Les dispositions sur la protection des renseignements personnels contenues dans la première partie de la LPRPDE sont les principes établis également dans le Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation[259]. Comme le Groupe de l'article 29 le fait remarquer : « ces dispositions ont été comparées à celles de la Directive (95/46/CE) »[260].

Le Canada dispose depuis 1985 d'une loi encadrant la protection des renseignements personnels pour le secteur public, ce qui ne fait que confirmer le caractère pionnier du pays dans cette matière.

---

[257] COMMISSION EUROPÉENNE, préc., note 255, point 9.
[258] C. CHASSIGNEUX, préc., note 233, p. 132.
[259] *Code type sur la protection des renseignements*, CAN/CSA-Q380-F96 (C2001).
[260] GROUPE « ARTICLE 29 » SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES, préc., note 253, p. 3.
Le Groupe de l'article 29 fait référence à comment cette analyse était déjà contenu dans ce document qu'ils ont adopté le 24 juillet 1998 : GROUPE « ARTICLE 29 » SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES, *Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la Directive communautaire sur la protection des données*, GT 12.

La LPRP « a pour objet de compléter la législation canadienne en matière de protection des renseignements personnels relevant des institutions fédérales et de droit d'accès des individus aux renseignements qui les concernent »[261]. Pour ce qui est de nos travaux, cette loi est celle que nous allons étudier plus en profondeur afin de comprendre comment les normes canadiennes en la matière vont s'appliquer au contexte de l'État en réseau.

Cette loi est, selon l'expert canadien David H. Flaherty « une maison vieille de 25 ans que l'on a peu entretenue et rénovée »[262] et qui sans aucun doute va devoir faire l'objet d'une réforme en profondeur afin de mettre à jour ses dispositions.

Voici l'idée que l'auteur canadien souligne à cet égard : « Si la Loi sur la protection des renseignements personnels constituait une déclaration progressiste en matière de protection de la vie privée au début des années 1980, c'est maintenant une loi dépassée qui ne réglemente plus convenablement la manière dont les institutions fédérales recueillent, utilisent, conservent et communiquent les renseignements personnels »[263].

Bien sûr, nombreux sont les arguments en faveur de la réforme de ce texte canadien – et nous y reviendrons dans les pages qui suivent –, cependant, pour ce qui est du sujet qui nous occupe, un des problèmes les plus urgents à résoudre quant à cette législation – et qui prouve qu'elle est désuète –, est que la LPRP ne répond pas à la « norme nationale canadienne » qui a été énoncée par le Parlement canadien dans la LPRPDE.

Nous pouvons identifier, comme certains experts l'ont fait, plusieurs principes de base de protection des renseignements personnels se trouvant dans la législation relative au secteur privé et qui sont absents dans la LPRP relative au secteur public.

---

[261] Article 2 de la LPRP.
La LPRP définit à son article 3 une « institution fédérale » comme étant tout ministère ou département d'État relevant du gouvernement du Canada, ou tout organisme, figurant à l'annexe.

[262] David H. FLAHERTY, *Réflexions sur la réforme de la Loi sur la protection des renseignements personnels*, Juin 2008, p. 4, en ligne : http://www.priv.gc.ca/information/pub/pa_ref_df_f.pdf (consulté le 13 mars 2011).

[263] *Id.*

Le CPVPC a expliqué que l'entrée en vigueur en 2001 de la LPRPDE a eu pour effet de mettre encore davantage en relief les lacunes de la loi régissant la protection des renseignements personnels dans le secteur public canadien : « Il est malheureux que les mesures de protection de la vie privée offertes aux Canadiennes et aux Canadiens soient plus efficaces pour les renseignements personnels détenus par le secteur privé que pour ceux qui se trouvent entre les mains du gouvernement »[264].

Ainsi, nous observons que le secteur privé doit se conformer d'une part, « à l'obligation d'obtenir le consentement pour accéder à de l'information » et, par ailleurs, est tenu « de maintenir des mécanismes de sécurité pour préserver les renseignements, ce dont on ne trouve aucun équivalent direct dans la Loi sur la protection des renseignements personnels (LPRP) »[265].
Ces deux principes essentiels dans la préservation de la confidentialité des renseignements personnels dans le contexte du secteur public sont absents de la LPRP, ce qui donne une idée des lacunes que ce texte comporte dans le contexte actuel et, plus particulièrement, pour ce qui est de la mise en place de l'administration électronique au Canada.

Mais David H. Flaherty va encore plus loin en affirmant que la LPRP « pèche contre huit des dix principes de la norme nationale du Canada[266] en matière de protection de la vie privée, soit au chapitre de la reddition de comptes, de la transparence, de la détermination des fins de la collecte, du consentement, de la limitation de l'utilisation, de la communication et de la conservation des renseignements personnels, des tests de qualité des données et des mesures de sécurité »[267].

---

[264] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2006-2007, Rapport concernant la Loi sur la protection des renseignements personnels*, 2007, p. 8.
[265] D. H. FLAHERTY, préc., note 262, p. 8.
[266] L'auteur fait ici référence aux principes qui ont été établis par la CSA et qui se trouvent dans l'Annexe 1 de la LPRPDE.
[267] D. H. FLAHERTY, préc., note 262, p. 43 et 44.

D'autres experts n'ont pas non plus hésité à dénoncer le besoin de renforcer les dispositions concernant la communication de renseignements personnels par le gouvernement canadien aux États étrangers[268].

Sans aucun doute, l'absence de principes basiques de protection des renseignements personnels est à l'origine d'une telle précarité dans la protection accordée aux renseignements personnels détenus par le secteur public. Nous observons, plus particulièrement, pour ce qui est des principes de traitement équitable de l'information qui sous-tendent la LPRP, qu'ils « comportent des lacunes et s'accompagnent de mécanismes de contrôle des pratiques de gestion de l'information de l'administration fédérale trop laxistes, voire inexistantes »[269].

Le CPVPC a également produit un Rapport[270] en 2006, qui a été présenté au Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, constituant un vaste plan de réforme de la LPRP[271]. Toutefois, il faut noter que depuis 1987 nous assistons à une demande généralisée quant à une réforme à caractère urgent de la LPRP, demande de réforme véhiculée par une succession d'examens, recommandations et rapports visant à exiger de la part du gouvernement une réforme, qui n'est jamais arrivée[272].

Bien sûr, nous retrouvons dans la LPRP des dispositions visant à protéger les renseignements personnels, répondant à l'esprit des principes présents dans la législation canadienne pour le secteur privé. Toutefois, nous observons également

---

[268] Voir à ce sujet : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Modifications immédiates proposées à l'égard de la Loi sur la protection des renseignements personnels*, Comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, le 29 avril 2008, p. 31 et s.

[269] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 264, p. 9 et 10.

[270] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Responsabilité du gouvernement en matière de renseignements personnels; Réforme de la Loi sur la protection des renseignements personnels*, juin 2006.

[271] Voir à ce sujet : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 264, p. 9.

[272] Voir sur l'historique des demandes de réforme de la LPRP : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 264, p. 15.

un vide juridique pour ce qui relève de certaines obligations présentes dans les législations européennes et dans la loi canadienne régissant le secteur privé. Nous analyserons plus tard dans quelle mesure l'esprit que le principe de finalité renferme se trouve présent dans les dispositions contenues dans la LPRP.

## SECTION 2 Le principe de finalité, pierre angulaire des systèmes de protection des renseignements personnels

Nous étudierons dans cette section dans quelle mesure le principe de finalité constitue la pierre angulaire des systèmes de protection des renseignements personnels et le rôle qu'il occupe dans le système basé sur les principes de protection. Nous analyserons également comment les différents textes, au Canada et en Europe, imposent la limitation des fins d'utilisation des renseignements personnels, afin de limiter les usages non autorisés, tant au secteur privé qu'au secteur public.

### 1- Le principe de finalité comme principe directeur dans le secteur public et privé

Nous avons pu constater que les instruments analysés protégeant les renseignements personnels, d'un côté et de l'autre de l'Atlantique, s'articulent autour de certains principes. Examinons maintenant comment le principe de finalité a été appréhendé par les différents législateurs, afin d'essayer de cerner les contours d'un tel concept.

Sur le plan européen, la première idée à souligner est que le principe de finalité constitue une des pierres angulaires de la Loi I et L, même si ce principe ne figurait pas très clairement dans le texte de 1978. Toutefois, nous retrouvons très vite l'expression de ce principe à la Convention 108, à la Directive 95/46/CE, ainsi que dans la Loi I et L modifiée.

#### A- La finalité dans la Convention 108 et la Directive 95/46/CE

Commençons par analyser la manière dont la Convention 108 a encadré ce principe. L'article 5 portant sur la « Qualité des données » affirme que les données à caractère personnel faisant l'objet d'un traitement automatisé sont « obtenues et traitées loyalement et licitement » (paragraphe 5(a)), que les données ne doivent être enregistrées qu'en vue de finalités déterminées et légitimes et qu'elles ne doivent pas être utilisées de manière incompatible avec celles-ci (paragraphe 5(b)),

qu'elles doivent être « adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées » (paragraphe 5(c)), qu'elles doivent être exactes et si nécessaire mises à jour (paragraphe 5(d)) et conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (paragraphe 5(e)).

Le Rapport Explicatif de la Convention 108 fournit des informations visant à nous faire comprendre certaines dispositions de cet instrument. Ainsi, il est expliqué que la référence aux « finalités » dans les paragraphes 5(b) et 5(c) indique qu'il ne sera pas permis d'enregistrer de données pour des finalités non déterminées, mais que la façon dont la finalité légitime est précisée peut varier selon le droit interne[273]. Nous constatons donc, qu'il existe un renvoi vers le droit interne pour ce qui est de la détermination de la légitimité des finalités.
Avant de passer à l'étude de la manière dont la Directive 46/95/CE encadre le principe de finalité, nous pensons qu'il est important de faire remarquer que les Lignes directrices régissant la protection de la vie privée et des flux transfrontières de données de caractère personnel de l'OCDE[274] établissent notamment dans leur principe relatif à la *qualité des données* que « les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour ».

Cet instrument établit, le *Principe de spécification des finalités* : «Les finalités en vue desquelles les données de caractère personnel sont traitées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui

[273] CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel du 28 janvier 1981 du Conseil de l'Europe*, point n. 41, en ligne: http://conventions.coe.int/Treaty/FR/Reports/Html/108.htm (consulté le 20 octobre 2010).
[274] OCDE, *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, adoptées le 23 septembre 1980. (ci-après : Lignes directrices de l'OCDE relatives à la protection de la vie privée).

ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées ». Cet instrument, même s'il n'a pas de nature contraignante, accorde une grande importance au fait de cerner toute la complexité du principe de finalité.

Nous retrouvons déjà dans les considérants de la Directive 46/95/CE des mentions explicites à l'égard du principe de finalité, en soulignant cette idée : « considérant que tout traitement de données à caractère personnel doit être effectué licitement et loyalement à l'égard des personnes concernées ; qu'il doit porter, en particulier, sur des données adéquates, pertinentes et non excessives au regard des finalités poursuivies ; que ces finalités doivent être explicites et légitimes et doivent être déterminées lors de la collecte des données ; que les finalités des traitements ultérieurs à la collecte ne peuvent pas être incompatibles avec les finalités telles que spécifiées à l'origine »[275].

Le Chapitre II de la Directive 95/46/CE, en faisant référence aux « Conditions générales de licéité des traitements de données à caractère personnel », établit à son article 5 que « les États membres précisent, dans les limites des dispositions du présent chapitre, les conditions dans lesquelles les traitements de données à caractère personnel sont licites ».

Nous observons encore, dans ce cas, un appel au droit interne pour ce qui est des conditions de licéité des traitements de données personnelles. La Section I du Chapitre II comporte les « Principes relatifs à la qualité des données » et nous présente un seul article imposant au sujet de la qualité des données, des principes tributaires du principe de finalité.

[275] Considérant 28 de la Directive 46/95/CE. Le considérant 29 de la Directive 95/46/CE vient compléter cette idée : « considérant que le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques n'est pas considéré en général comme incompatible avec les finalités pour lesquelles les données ont été auparavant collectées, dans la mesure où les États membres prévoient des garanties appropriées ; que ces garanties doivent notamment empêcher l'utilisation des données à l'appui de mesures ou de décisions prises à l'encontre d'une personne ».

Comme certains le font remarquer, l'article 6 de la Directive 95/46/CE contient trois types de dispositions : « des principes généraux relatifs à la qualité des données, des prescriptions imposées au responsable du traitement, et enfin des dispositions particulières relatives à la conservation et au traitement des données à des fins historiques, statistiques ou scientifiques »[276].

Ainsi, l'article 6 invite les États membres à prévoir que les données à caractère personnel soient « a) traitées loyalement et licitement ; b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités ». Cet article établit par la suite qu'« un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées ».
Cet article 6 oblige également à que les données à caractère personnel soient : « c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ultérieurement ; d) exactes et, si nécessaire, mises à jour, toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ». L'article 6 impose aussi que les données soient « e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour que les données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques ».

Cette disposition finit par énoncer au paragraphe 2 qu' «il incombe au responsable du traitement d'assurer le respect du paragraphe 1», en faisant reposer cette responsabilité dans cette figure.

[276] G. BRAIBANT, préc., note 56, p. 52.

Nous pouvons observer comment l'alinéa 6 (1)c) établit un principe de proportionnalité entre la qualité des données et la finalité de leur traitement, très similaire à celui qui se trouve dans le paragraphe 5(c) de la Convention 108 et qui, par contre, n'était pas explicite dans la Loi I et L. Toutefois, nous avons pu constater que le principe de finalité a inspiré dès l'origine la jurisprudence de la CNIL, « tant dans les formalités préalables à la création des traitements publics que dans les contrôles *à posteriori* »[277].

Selon certains auteurs, pour ce qui est de la Loi I et L avant sa modification, si la loi ne fait pas « expressément mention du principe de finalité, elle en fait une application partielle en imposant que soit indiquée la finalité du traitement dans les déclarations (…) et en sanctionnant pénalement le détournement de finalité (…) »[278]. En effet, la Loi I et L comportait déjà des dispositions faisant référence à la finalité des traitements uniquement de manière incidente, ce qui n'a pas empêché la CNIL d'estimer en 1985 que cette dimension devrait davantage être prise en compte dans le futur[279].

Le Rapport Braibant signale que l'énoncé de principes généraux relatifs à la qualité des données de l'article 6 de la Directive 95/46/CE ne devait pas être repris littéralement dans la loi française à l'heure de la transposition du texte européen, puisqu'il était partiellement redondant avec certaines règles développées dans d'autres articles de la Directive[280].

---

[277] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *6e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1985, p. 213.

[278] G. BRAIBANT, préc., note 56, p. 15.

[279] COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS, préc., note 277, p. 213.

[280] G. BRAIBANT, préc., note 56, p. 52.
Voici l'idée que nous retrouvons dans ce rapport cité quant au contenu de l'article 6 de la Directive 46/95/CE : « Ainsi le point a) ne fait-il que renvoyer d'une part aux conditions générales de licéité des traitements développés dans l'article 7, et d'autre part à l'obligation – dictée par les articles 10 et 11, paragraphe 1 – d'informer les personnes concernées au moment de la collecte ou de la première communication á des tiers ».

L'alinéa 6(b)1) constitue une innovation majeure de la Directive 46/95/CE, en posant le principe de finalité, qui selon certains devait être repris dans la Loi I et L modifiée. Et cela, dans la mesure où « il est une condition de la licéité de la collecte des données (la finalité du traitement doit en effet être déterminée dès le stade de la collecte), et où il pose une exigence de compatibilité entre la finalité de la collecte et celles des traitements ultérieurs »[281].

Pour ce qui est de l'alinéa 6(1)c), il « dérive de ce principe de finalité une règle de proportionnalité »[282], quand il précise que les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées ou pour lesquelles elles seront traitées ultérieurement, pouvant observer que les trois adjectifs sont « largement synonymes »[283]. Nous identifions également le principe d'exactitude des données qui est repris par le paragraphe 6(4).

Nous observons également que de l'alinéa 6(1)d) et du paragraphe 6(2) dérivent des prescriptions imposées au responsable du traitement : d'une part, l'obligation de prendre toutes les mesures raisonnables pour que les données inexactes ou incomplètes, au regard des finalités[284] pour lesquelles elles ont été collectées ou pour lesquelles elles seront traitées ultérieurement, soient effacées ou rectifiées ; et, d'autre part, la responsabilité générale du respect des principes énoncés au paragraphe 6(1).

Le Rapport Braibant a examiné également ces dispositions visant à assurer le principe de finalité et imposant des obligations au responsable du traitement et a fait remarquer que la référence « mesures nécessaires » paraissait plus claire en droit français que la notion « *reasonableness* » propre au droit anglo-saxon, en ajoutant « qu'il appartiendra à l'autorité de contrôle et au juge de déterminer les

[281] G. BRAIBANT, préc., note 56, p. 52.
[282] *Id.*, p. 53. Voir également les travaux préparatoires de la Loi I et L modifiée et plus concrètement, ceux du Sénat, en première lecture quant au Rapport nº 218 de M. Alex Türk dans sa partie relative à l'article 6 modifié de la loi du 6 janvier 1978 et les conditions de collecte et de traitement.
[283] *Id.*
[284] Nous soulignons.

circonstances qui permettront d'exonérer le responsable de ses obligations en la matière »[285].

Nous constatons ici encore que l'utilisation de ce type de recours de la part du législateur offre la possibilité d'apprécier au cas par cas l'adéquation au texte de loi, ce qui comporte également une difficulté évidente. Il reste à voir en effet si l'expression adoptée faisant référence à ce qui est « nécessaire » est plus claire que celle relative à ce qui est « raisonnable » et que nous retrouvons dans d'autres instruments législatifs.

Certains précisent que « bien que les critères de la finalité tels que posés par la directive soient déjà mis en application par la CNIL, il semble opportun de profiter du travail de transposition de la directive pour inscrire le principe fondamental de finalité du traitement dans la loi française »[286].

### B- La Loi I et L modifiée et le principe de finalité

La Loi I et L modifiée est venue corriger la situation existante avant son adoption et affirme, en énonçant dans son article 6 le principe de finalité, être une des conditions devant être satisfaites lors de la création d'un traitement : « Un traitement ne peut porter que sur des données à caractère personnels qui satisfont aux conditions suivantes : 1. Les données sont collectées et traitées de manière loyale et licite ; 2. Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus (….)[287] et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ; 3. Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ; 4. Elles sont exactes, complètes et, si

[285] G. BRAIBANT, préc., note 56, p. 53.
[286] P. BLANC-GONNET, préc., note 38, p. 71.
[287] L'article fait référence au « respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X ».

nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ; 5. Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ».

Nous observons que la loi énonce un principe d'interdiction de traitement ultérieur des données qui serait incompatible avec ses finalités, afin d'écarter le risque d'une utilisation injustifiée des données personnelles, même de manière décalée dans le temps, mais sans aller plus loin dans l'élaboration de ce que la loi considère comme « incompatible ».
Nous constatons alors que la Loi I et L a repris le terme « ultérieur », comme l'avait fait la Directive 46/95/CE, même si la CNIL avait montré son désaccord lors de la rédaction de l'avis qu'elle a produit par rapport à la Loi I et L modifiée :

> « Cette rédaction qui reprend celle de la directive est susceptible de soulever des difficultés dans la mesure où l'emploi de l'adverbe ultérieurement paraît autoriser la collecte de données qui seraient dépourvues de pertinence ou excessives au regard de la finalité du traitement initial au motif que de telles données deviendraient pertinentes au regard d'un traitement ultérieur, par exemple, un traitement statistique ou scientifique. Le contrôle de la pertinence s'en trouverait donc considérablement relâché. »[288]

Pour cela, la CNIL envisage plutôt, sans s'éloigner de la Directive 46/95/CE et en s'inspirant du paragraphe 5 c) de la Convention 108, un article précisant tout simplement que les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées. Nous constatons toutefois que, dans la rédaction finale de la Loi I et L modifiée, à l'image de la Directive 46/95/CE, l'adverbe « ultérieur » a finalement été adopté.

[288] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 235, p. 26 (nous soulignons).

Ce principe s'accompagne d'une exception importante pour ce qui relève des traitements statistiques et de recherche scientifique ou historique, en affirmant que des utilisations de cette nature sont envisageables si elles s'effectuent dans les conditions établies par la loi et si elles ne servent pas à prendre des décisions à l'égard des personnes.
La finalité est l'une des informations devant être présentes dans la déclaration ou la demande d'autorisation de fichier, comme établi au paragraphe 30.2 de la Loi I et L modifiée.

Nous observons ainsi que la structure du traitement de données à caractère personnel, ainsi que les conditions de sa mise en œuvre vont dépendre de la finalité de celui-ci. Mais de la finalité vont dépendre également les données personnelles qu'il sera possible de collecter, les destinataires habilités à recevoir communication des données, ainsi que la durée de conservation de ces données, puisque c'est au regard de la finalité du traitement que sera jugé le traitement dans son ensemble[289].

Il faut noter également que le non-respect du principe de finalité est prévu, par l'article 226-21 du Code pénal[290], grâce à une sanction en cas de détournement des données personnelles de leur finalité déclarée initialement.

Pour ce qui est du concept d'extension de finalité et l'utilisation ultérieure des données personnelles, nous observons que, dès les débats en séance publique de ce texte, cette question était au centre des préoccupations à l'heure de décider de l'adoption d'un amendement à l'article 6 : « cet amendement vise à garantir l'effectivité du principe de finalité qui est au cœur du dispositif de protection des

[289] Voir à ce sujet : Marie-Laure LAFFAIRE, *Protection des données à caractère personnel*, Éditions d'organisation, Paris 2005, p. 65.
[290] Cet article du Code Pénal français dispose que « Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende ».

personnes physiques à l'égard des traitements des données à caractère personnel. Il convient en effet de conférer un caractère exceptionnel à une réutilisation ultérieure de ces données pour une finalité autre que celle initialement retenue »[291].
Il s'agissait d'insérer le mot « seul », après le mot « toutefois » au paragraphe 6.2, afin de circonscrire l'utilisation ultérieure des données aux cas de statistiques ou de recherche scientifique ou historique[292]. Voici comment cela a été exposé : « Nous souhaitons conférer un caractère exceptionnel à une réutilisation ultérieure de ces données pour une finalité autre que celle initialement retenue, en la limitant à l'exception prévue par l'article 6 modifié de la loi »[293].

Le rapporteur, lors de cette séance publique, a montré le désaccord de la CNIL à cet amendement, surtout parce qu'une telle mesure paraissait véritablement excessive par rapport à l'enjeu et parce qu'ils avaient « bien insisté dans la discussion générale sur la nécessité de se référer chaque fois que possible aux principes de finalité et de proportionnalité ».

Il faut savoir que, si cet amendement avait été adopté, la « compatibilité » entre finalités aurait pu rester réduite uniquement et exclusivement à ce type de traitements ultérieurs (fins statistiques, fins de recherche scientifique ou historique), ce qui aurait pu avoir pour résultat, entre autres, le fait de limiter également la recherche en général.

Toujours au Sénat, mais en deuxième lecture, nous retrouvons cette idée dans le Rapport présenté : « l'article 6 reprendra l'essentiel des dispositions de la loi du 6 janvier 1978 déterminant les règles fondamentales de licéité des traitements des informations nominatives (notamment le respect des principes de loyauté et

---

[291] *Extraits des débats au Sénat*, première lecture de la Loi I et L modifiée, Séance publique du 1er avril 2003. Propos soutenus par M. Robert Bret quant à l'article 6 de la Loi I et L modifiée.
[292] La rédaction proposée était celle-ci : « Toutefois, "seul" un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données ».
[293] *Extraits des débats à l'Assemblée nationale*, deuxième lecture de la Loi I et L modifiée, Séance publique du 29 avril 2004. Propos soutenus par M. Frédéric Dutoit.

d'exactitude), tout en les complétant par les nouveaux principes de proportionnalité et de finalité issus de la directive »[294].

Lors des débats en séance publique[295] la question de mieux encadrer le principe de finalité, surtout en ce qui concerne les utilisations futures des données collectées, avait été soulevée en proposant que, pour respecter les principes de pertinence et d'adéquation entre autres, les finalités de réutilisation[296] soient précisées.

Le rapporteur a appuyé l'idée qu'il « vaut mieux laisser la CNIL intervenir au cas par cas »[297], en soulignant encore une fois l'importance de l'appréciation au cas par cas de la possibilité d'une utilisation ultérieure des données et cela, grâce aux principes de finalité et de proportionnalité.

Nous constatons alors que, dans la rédaction finale de la Loi I et L modifiée, on a voulu que les principes de finalité et de proportionnalité servent au décideur, à la CNIL ou au juge, pour évaluer une situation déterminée plus ou moins complexe et toujours « unique », puisque pour chaque traitement, une solution particulière d'encadrement devrait être mise en place.

Disons que le législateur a décidé de placer ces principes au cœur de la régulation Informatique et Libertés, principes devant être utilisés dans le processus d'appréciation au cas par cas, à la place d'établir des prescriptions ou interdictions ne couvrant que des situations très particulières.

Lors des débats en séance publique à l'Assemblée nationale française, nous assistons également à un débat fort intéressant sur la rédaction finale de cet article 6, qui montre une fois encore, la nette volonté de laisser à la CNIL la tâche d'analyser et d'examiner au cas par cas le respect du principe de finalité.

---

[294] *Extraits du Rapport nº 367 de M. Alex Türk*. Sénat, deuxième lecture de la Loi I et L modifiée.

[295] *Extraits des débats au Sénat*, deuxième lecture de la Loi I et L modifiée, Débats en séance publique du 15 juillet 2004.

[296] Nous soulignons.

[297] *Extraits des débats au Sénat*, deuxième lecture de la Loi I et L modifiée, Séance publique du 15 juillet 2004. Propos soutenus par M. Alex Türk.

Ainsi, il s'agit à cette occasion de tenir compte de la « très forte valeur informationnelle que peut générer une interconnexion de fichiers »[298], en faisant un lien très clair entre le respect du principe de finalité et le phénomène des interconnexions. Voici l'idée exprimée sur cette problématique :

> « Pour être effectifs, les principes de finalité du paragraphe 2) de cet article (article 6 de la Loi I et L modifiée), qui interdit une utilisation des données récoltées pour une finalité différente doivent être garantis par les conditions dans lesquelles s'effectueront de telles connexions : c'est pourquoi nous vous proposons que celles-ci soient effectuées par un tiers n'ayant pas intérêt à une telle connexion. (…) Monsieur le Rapporteur, vous nous dites que la CNIL a le pouvoir d'encadrer les conditions de ces interconnexions ; mais il vaudrait mieux l'inscrire dans la loi du 6 janvier 1978. Le recours à un tiers de confiance, n'ayant pas d'intérêt à cette interconnexion, est la condition pour empêcher les abus et offrir des garanties suffisantes aux personnes. »[299]

Un avis défavorable a été émis par le Rapporteur en ce qui concerne cet amendement, il a qualifié ce système d'extrêmement lourd et, même s'il a trouvé que l'idée était judicieuse, a affirmé « qu'il revient à la CNIL d'analyser chaque cas et de voir s'il convient de recourir au tiers de confiance. Faisons confiance à la CNIL »[300].

Nous observons alors que les dangers potentiels liés au phénomène des interconnexions, et pouvant conduire au non-respect du principe de finalité, justifient la volonté d'intégrer dans le texte de loi des garanties s'appliquant à l'ensemble des interconnexions. Et nous retrouvons encore une fois une réponse accordant à la CNIL la capacité de fixer au cas par cas les conditions dans le cadre de chaque interconnexion. Cela laisse « ouvertes » dans le texte de loi les

---

[298] *Extraits des débats au Sénat*, deuxième lecture de la Loi I et L modifiée, Séance publique du 15 juillet 2004. Propos soutenus par M. Charles Gautier.
[299] *Extraits des débats au Sénat*, deuxième lecture de la Loi I et L modifiée, Séance publique du 15 juillet 2004. Propos soutenus par M. Robert Bret.
[300] *Extraits des débats au Sénat*, deuxième lecture de la Loi I et L modifiée, Séance publique du 15 juillet 2004. Propos soutenus par M. Alex Türk.

différentes options visant à assurer le principe de finalité et ne limitant pas celles-ci au recours à un tiers de confiance.

Le considérant 53 de la Directive 46/95/CE souligne l'idée que « certains traitements sont susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat ou du fait de l'usage d'une technologie nouvelle ; qu'il appartient aux États membres, s'ils le souhaitent, de préciser dans leur législation de tels risques ».
Le considérant 54 établit également que « considérant que, au regard de tous les traitements mis en œuvre dans la société, le nombre de ceux présentant de tels risques particuliers devrait être restreint ; que les États membres doivent prévoir, pour ces traitements, un examen préalable à leur mise en œuvre, effectué par l'autorité de contrôle (…) ».
Notons que certains ont souligné en analysant le considérant 53 de la Directive 46/95/CE que le principe de finalité devait demeurer au centre de la nouvelle législation en France, au détriment de certaines expressions que la Directive 46/95/CE introduit : « Si cette rédaction (celle du considérant 53 de la Directive 46/95/CE) peut se prévaloir de la directive, elle n'en introduit pas moins des notions imprécises en droit français. En effet, si le terme "finalités" est familier en droit des données à caractère personnel, tel n'est malheureusement pas le cas de ceux se référant à la "nature" ou à la "portée" des traitements »[301].

Ainsi, le paragraphe 25.1 conditionne la mise en œuvre de certains traitements à l'obtention d'une autorisation de la CNIL, par l'énumération de certaines catégories de traitements en se fondant d'une part, sur la nature des données concernées et, d'autre part, sur la finalité des traitements[302].

[301] *Extraits du Rapport nº 1537 de M. Francis Delattre*. Assemblée Nationale, deuxième lecture de la Loi I et L modifiée.
[302] *Extraits du Rapport nº 218 de M. Alex Türk*. Sénat, première lecture de la Loi I et L modifiée.

Nous retrouvons dans cette catégorie répondant à la finalité du traitement, premièrement le cas des « traitements automatisés susceptibles, du fait du leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire » (alinéa 25.1)4))

Mais nous retrouvons également l'alinéa 25.1)5) faisant mention spécifique au principe de finalité, notamment pour ce qui est de l'encadrement des interconnexions, présentées dans la Loi I et L modifiée comme un phénomène présentant des risques particuliers. Ainsi, cet article fait référence aux « Traitements automatisés ayant pour objet :

- l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ;
- l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ».

Il faut se rappeler que la CNIL avait déjà, en 1996, retenu ces deux catégories et bien d'autres à l'heure d'identifier des traitements comportant des risques particuliers[303]. Pour ce qui est des interconnexions déjà identifiées dans cette liste, certains ont affirmé, avant même la transposition en droit français de la Directive 95/46/CE, que « les interconnexions sont multiples à l'intérieur d'une même administration et d'une même entreprise et beaucoup ne sont pas dangereuses »[304], et qu'il faudrait limiter le champ des autorisations aux interconnexions de traitements à finalités différentes gérées par des organismes distincts, afin d'assurer la protection des données personnelles.

[303] Dans une délibération du 14 mai 1996 la CNIL établit une liste comprenant 11 rubriques où se trouvent déjà les « interconnexions entre fichiers distincts » et « l'exclusion des personnes d'un droit, d'une prestation ou d'un contrat ».
Voir à ce sujet : Danièle BOURCIER, « De l'intelligence artificielle à la personne virtuelle : émergence d'une entité juridique? », *Droit et société*, 2001/3, n. 49, 847, p. 863.
[304] G. BRAIBANT, préc., note 56, p. 74 et 75.

La CNIL, dans son Avis sur le Projet de loi modifiant la Loi du 6 janvier 1978[305], dénonçait une rédaction de la Loi I et L modifiée créant la possibilité de que la procédure d'autorisation s'applique uniquement à la double condition que les fichiers interconnectés aient des finalités distinctes et qu'ils soient gérés par des organismes distincts. La CNIL affirme :

> « Une telle rédaction pourrait donner à penser que toute personne publique ou privée pourrait interconnecter tous les fichiers dont elle dispose, quelle que soit leur finalité (ainsi une préfecture ou une collectivité locale) et être ainsi la porte ouverte à tous les safaris locaux : elle mérite pour ce motif d'être revue. »[306]

Elle rappelle à cet effet que le principe de finalité des fichiers « paraît commander que toute interconnexion entre des fichiers à finalité distincte, même s'ils sont mis en œuvre par un même organisme, fasse l'objet d'un examen préalable »[307].
Mais il est également proposé de subordonner à l'autorisation de la CNIL les traitements automatisés incluant « les rapprochements, l'interconnexion ou toute autre forme de mise en relation des données avec d'autres données pour des finalités différentes »[308].
Afin d'éviter de potentiels problèmes de précision dans l'interprétation de la loi, la CNIL a encore recommandé de renoncer à l'expression de « finalité principale du traitement »[309], susceptible d'interprétation en appuyant cette observation sur le fait que la Directive 95/46/CE ne retient pas une telle expression.

Une autre des questions importantes pour le législateur français est de déterminer qui aurait le pouvoir d'accorder l'autorisation nécessaire à la mise en œuvre de ces traitements. Le Rapport Braibant a recommandé que ce soit la CNIL, puisqu'elle

---

[305] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 235, p. 7.
[306] *Id.*
[307] *Id.*
[308] *Id.*
[309] *Id*.

est la mieux placée pour se prononcer et, parce que la Directive 95/46/CE le permet, celle qui peut avoir ce pouvoir d'autorisation[310].

### C - Le secteur public canadien

Nous tenterons par la suite d'identifier, sur le plan fédéral canadien, les dispositions dans les lois relatives à la protection des renseignements personnels faisant référence à la notion de finalité, ainsi qu'aux dispositions encadrant les fins pour lesquelles les renseignements personnels peuvent être recueillis, utilisés et communiqués par les organismes publics.
Nous analyserons les dispositions de la LPRP s'appliquant au secteur public fédéral et pouvant avoir une incidence majeure sur la mise en place d'un gouvernement électronique.

#### i) La notion de la finalité et la LPRP

Il faut avant tout noter, comme D. Flaherty l'a fait, que l'un des problèmes posés par la LPRP aujourd'hui est qu'il devient difficile de retracer dans son libellé les principes de protection des renseignements personnels que nous retrouvons dans la LPRPDE et dans le code de la Canadian Standards Association [311]. Par conséquent, « cet état des choses invite à appliquer, dans une version révisée de la LPRP, une approche davantage fondée sur les principes que ce n'est le cas actuellement »[312].
Notre objectif le plus important est d'identifier et d'analyser les dispositions de la LPRP ayant un lien avec le principe de finalité. L'article 4 de la LPRP établit que « les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou activités », en affirmant le

[310] G. BRAIBANT, préc., note 56, p. 77.
Voir également à ce sujet : *Extraits du Rapport n° 218 de M. Alex Türk*. Sénat, première lecture de la Loi I et L modifiée.
Il faut souligner que cette solution avait un précédent, puisque la Loi de bioéthique du 1er juillet 1994 avait déjà confié à la CNIL le pouvoir d'autoriser par elle-même les « traitements automatisés de données nominatives ayant pour fin la recherche dans le domaine de la santé ».
[311] Ci-après : CSA.
[312] D. H. FLAHERTY, préc., note 262, p. 19.

principe selon lequel un organisme public ne peut recueillir que des renseignements personnels qui sont nécessaires à son activité.

Comme K. Benyekhlef le précise, le législateur fédéral n'a pas voulu exclure spécifiquement certains types de données dites sensibles et nous ne retrouvons donc pas dans la LPRP une mention explicite du « Principe de la justification sociale »[313]. D'après ce principe, on ne pourrait pas procéder à la collecte de certaines données personnelles sensibles, « en d'autres termes, on ne recueillerait des données personnelles que pour des objectifs socialement acceptables »[314]. Nous avons pu constater dans les pages précédentes que la Directive 95/46/CE à son article 8 et la Loi I et L modifiée dans ses articles 8 à 10 contiennent des « Dispositions propres à certaines catégories de données » et, en fonction de leur degré de sensibilité, comportent des exclusions de principe quant à certains types de données.

En effet, le législateur canadien a voulu conditionner la collecte de renseignements uniquement à l'établissement d'un lien entre celle-ci et la mission de l'institution fédérale qui procède à cette collecte[315]. Un organisme public canadien pourra donc uniquement recueillir les informations nécessaires à ses tâches dans le développement de son activité.
Le CPVPC a présenté une liste de modifications immédiates proposées à l'égard de la LPRP et il est important de souligner que la première de ces recommandations fait directement référence à cet article 4 de la LPRP. Le CPVPC considère, pour ce qui est du contenu de l'article 4, « qu'une façon beaucoup plus efficace d'assurer le droit à la vie privée, conformément aux lois modernes en matière de protection des données, consiste à exiger que les institutions recueillent seulement les

[313] Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Éditions Thémis, Montréal, 1992, p. 100.
[314] *Id.*
[315] *Id.*

renseignements qui sont nécessaires et raisonnables dans le contexte de leurs programmes et activités »[316].

La proposition du CPVPC vise notamment à établir un « test de la nécessité » par la voie législative, afin que les institutions gouvernementales qui recueillent des renseignements personnels soient obligées de démontrer la nécessité de recueillir ces renseignements. Il semble clair que, aujourd'hui, le seul établissement d'un lien entre les renseignements personnels et la mission de l'institution fédérale qui procède à la collecte semble insuffisante aux yeux du CPVPC qui fait alors appel au critère de la nécessité.

K. Benyekhlef nous rappelle, en 1992, une idée centrale dans le contexte de nos travaux : « En effet, une utilisation non conforme à la mission confiée à l'organisme recueilleur est contraire, comme nous le savons, au principe de finalité ».[317]Nous observons qu'actuellement le principe de finalité est de plus en plus lié à d'autres critères, tels que la « nécessité » et le « raisonnable », pour la récolte des renseignements ayant un lien direct avec les activités d'un organisme public, et cela afin d'assurer plus efficacement le droit à la vie privée.

Ainsi, à titre d'exemple, notons que le principe 4.4 de l'Annexe 1 de la LPRPDE limite la collecte des renseignements personnels à ceux « nécessaires aux fins déterminées » et la Loi sur le service canadien du renseignement de sécurité[318] à son article 12 limite la collecte des renseignements personnels à ceux « nécessaires aux fins déterminées »[319].

Le CPVPC nous rappelle que presque toutes les provinces et tous les territoires du Canada disposent d'un modèle législatif encadrant le secteur public qui va imposer

[316] COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 268, p. 7 (nous soulignons).
[317] Karim BENYEKHLEF, préc., note 313, p. 107.
[318] L.R.C. 1985, c. C-23.
[319] Voir à ce sujet : COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 268, p. 7. Le CPVPC donne à titre d'exemple ces deux dispositions présentes dans les lois canadiennes.

au moins une de ces trois conditions. Ainsi, nous remarquons : 1) que la collecte doit expressément être autorisée par un texte législatif ; 2) que les renseignements doivent être recueillis aux fins de l'application de la loi ; c) que les renseignements doivent être directement liés et nécessaires à un programme ou à une activité de l'organisme public en question.

Le CPVPC justifie sa demande d'inclusion du « test de la nécessité » dans le texte de loi en affirmant que le libellé actuel de l'article 4 établit une norme qui n'est pas à la mesure des droits fondamentaux au cœur de la LPRP et recommande également de combiner cette réforme du texte au fait de permettre à une personne de contester devant les tribunaux tout ce qui concerne la collecte, l'utilisation et la communication de ses renseignements personnels, afin de créer un cadre juridique plus approprié pour le secteur public [320].

La LPRP oblige également les institutions fédérales à recueillir auprès de l'individu lui-même, chaque fois que possible, les renseignements personnels destinés à des fins administratives le concernant, sauf autorisation contraire de l'individu ou autres cas d'autorisation prévus au paragraphe 8(2), que nous étudierons dans les pages qui suivent (paragraphe 5(1)).

Les institutions fédérales canadiennes sont tenues également d'informer l'individu du fait qu'elle recueille des renseignements personnels le concernant ainsi que des fins auxquelles ces renseignements le concernant sont destinés (paragraphe 5(2))[321]. Comme certains l'ont souligné, le « principe de la limitation de la collecte » obligeant à ce que la collecte des renseignements personnels se fasse par des moyens licites et loyaux est uniquement énoncé à cet article 5 de la LPRP de façon implicite[322].

[320] *Id.*, p. 8.
[321] L'article 5 paragraphe 3 établit que les paragraphes (1) et (2) ne s'appliquent pas dans les cas où leur observation risquerait : a) soit d'avoir pour résultat la collecte de renseignements inexacts; b) soit de contrarier les fins ou de compromettre l'usage auxquels les renseignements sont destinés.
[322] K. BENYEKHLEF, préc., note 313, p. 113.

Il est pareillement important, dans le contexte canadien, d'analyser les concepts de « fin administrative» et celui de « fin non administrative ». Ainsi, le Secrétariat du Conseil du Trésor[323] définit le « fin administrative » comme un processus de prise de décision qui touche directement la personne[324]. Le SCT souligne que cette définition comprend en outre toute utilisation des renseignements personnels afin de confirmer l'identité d'une personne ou de déterminer si celle-ci est admissible aux programmes gouvernementaux[325].

Le SCT va définir les « fins non administratives » comme étant l'utilisation de renseignements personnels pour une fin qui n'est pas liée à une décision touchant directement à la personne, ce qui englobe notamment l'utilisation des renseignements personnels à des fins de recherche, de statistique, de vérification et d'évaluation[326].

Comme le CPVPC nous le rappelle, ces dispositions de la LPRP ne s'appliquent pas aux renseignements personnels recueillis par le gouvernement à des fins non administratives, même si ces fins peuvent affecter une personne ou le groupe de personnes auquel elle appartient. En conséquence, le CPVPC préconise que la LPRP puisse se doter d'un cadre applicable également aux renseignements personnels recueillis à des fins non administratives[327].

Pour ce qui est du paragraphe 5(1), qui autorise le responsable d'un organisme fédéral à décider à sa discrétion de recueillir directement ou indirectement en appliquant de manière sélective le critère de « mesure du possible », le CPVPC préconise d'autres modifications. Ainsi, il a été conseillé que cette disposition

---

[323] Secrétariat du Conseil du Trésor. (ci-après : SCT).

[324] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Responsabilité du gouvernement en matière de renseignements personnels, Réforme de la Loi sur la protection des renseignements personnels*, juin 2006, p. 29.

[325] Voir cette définition : SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Politique sur la protection de la vie privée*, 2008, en ligne : http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510 (consulté le 20 octobre 2010).
Il faut noter que cette version de cette Politique est entrée en vigueur le 1er avril 2008 et elle remplace celle de 1993 ainsi que toutes les obligations politiques contenues dans les rapports de mise en œuvre diffusées jusqu'à la date de son entrée en vigueur.

[326] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 325.

[327] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 324, p. 29.

indique clairement qu'une institution est tenue de recueillir les renseignements qui seront utilisés à des fins administratives directement auprès de la personne concernée, sauf autorisation prévue dans les exceptions claires et précises énoncées dans la LPRP.

De même, le paragraphe 5.2 présente, selon le CPVPC, une vision très atténuée du droit fondamental à la protection de la vie privée, qui devrait être élargie « afin d'exiger que les institutions gouvernementales précisent sous quelle autorité les renseignements sont recueillis, l'utilisation qui en sera faite, les institutions avec lesquelles ils seront échangés, les conséquences d'un refus de les fournir et le droit des personnes concernées de déposer une plainte en vertu de la LPRP »[328].

Comme nous pouvons le constater, des modifications potentielles de la LPRP touchent directement à la question concernant la protection accordée aux renseignements personnels en fonction des fins pour lesquelles les renseignements peuvent être utilisés, mais servent également à exiger des organismes publics de préciser l'utilisation qui sera faite de ces renseignements personnels et de communiquer à la personne concernée les institutions avec lesquelles les informations seront échangées.
Le principe de finalité demeure donc au centre des débats pour ce qui est de la réforme urgente de la LPRP dans le contexte du secteur public canadien.

Les articles 7 et 8 de la LPRP encadrent l'usage et la communication des renseignements personnels relevant des institutions fédérales. Nous observons un principe général selon lequel les renseignements personnels ne doivent être utilisés qu'aux fins prévues par la LPRP et ne peuvent être communiqués que conformément à la loi.

[328] *Id*.

ii) L'utilisation des renseignements personnels dans la LPRP

Les articles 7 et 8 de la LPRP stipulent que ces renseignements personnels peuvent être utilisés ou communiqués par une institution fédérale, sans le consentement de l'individu, à des fins directement rattachées aux fins pour lesquelles ces renseignements ont été recueillis ou consignés.

Nous observons également que le consentement de la personne concernée supprime l'obligation de se prévaloir d'une disposition d'usage ou de communication en vertu de l'article 7 ou 8 de la LPRP.

L'article 7 de la LPRP établit qu'à défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci :

> « a) qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution, de même que pour les usages qui sont compatibles avec ces fins [329] ;
> b) qu'aux fins auxquelles ils peuvent lui être communiqués en vertu du paragraphe 8(2). »

Le paragraphe 7(a) de la LPRP reprend d'une certaine façon le « principe de spécification des finalités » quand il remplit la fonction visant à empêcher que l'organisme recueilleur puisse modifier indûment les finalités pour lesquelles les données nominatives ont été recueillies[330]. Certains notent à propos de cette fonction du « principe de la spécification des finalités » constituant un élément du principe de finalité :

> « Autrement dit, l'organisme ne peut décider d'utiliser les données stockées pour des fins autres que celles spécifiées avant la collecte. Cet énoncé est cependant sujet à des exceptions. En effet, il est possible d'imprimer de nouvelles finalités à un ensemble de renseignements nominatifs si celles-ci ne sont pas incompatibles avec les finalités initiales. Ce critère de compatibilité, proposé par les Lignes directrices de l'OCDE, doit certainement s'apprécier à la

[329] Nous soulignons.
[330] Voir à ce sujet : K. BENYEKHLEF, préc., note 313, p. 118 et 119.

> lumière de toutes les circonstances et reposer sur une analyse de la raisonnabilité du lien entre les anciennes et les nouvelles finalités. Un changement de finalités peut s'exercer lors d'une communication de données à un organisme tiers. Cette question est intimement liée au principe de la limitation de l'utilisation (...). »[331]

En effet, la LPRP va introduire le « critère de compatibilité » entre les finalités, critère qui cause de nombreuses difficultés à l'heure de déterminer quand la finalité initiale sera compatible avec des usages ultérieurs de ces renseignements personnels. Nous observons que la doctrine lie cette évaluation au cas par cas au « critère du raisonnable » du lien entre les anciennes et les nouvelles finalités ainsi que la claire référence à la manière dont un changement de finalité pourrait se produire, lors d'une communication des renseignements personnels.

L'article 8 de la LPRP encadre la communication des renseignements personnels et établit une liste fermée des cas d'autorisation de communication des renseignements relevant d'une autorité fédérale.

La doctrine du SCT est la même pour ce qui est de l'usage et de la communication des renseignements personnels et, dès lors, concernant les articles 7 et 8 de la LPRP, le SCT qualifie d'« usages compatibles » aux « fins connexes » ou « fins directement rattachées » aux fins pour lesquelles les renseignements ont été recueillis[332].

Observons ici les différentes façons d'appréhender un même phénomène, faisant parfois appel à des notions telles que la « compatibilité » et d'autres fois faisant référence à la « connexion » ou au « rattachement » entre les finalités.

La doctrine du SCT va encore plus loin en affirmant que « pour qu'un usage ou une communication soit compatible, il doit avoir un lien pertinent et direct avec les fins premières pour lesquelles ces renseignements ont été recueillis ou consignés »[333].

---

[331] *Id.*, p. 119 (nous soulignons).

[332] SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Usage et communication de renseignements personnels*, 1993, en ligne : http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/CHAP2_4-2-fra.asp (consulté le 13 novembre 2010).

[333] *Id.*

C'est une des questions les plus problématiques pour ce qui est de la réutilisation des renseignements personnels dans le contexte fédéral canadien. Nous aurons l'occasion d'analyser dans les pages qui suivent la doctrine du CPVPC et du SCT quant à la façon de déterminer quels sont les « usages compatibles » et les critères à utiliser dans cette détermination.

iii) La communication de renseignements personnels dans la LPRP

L'article 8[334] de la LPRP encadre la communication des renseignements personnels et établit la règle générale selon laquelle les renseignements personnels qui relèvent

[334] 8. (1) Les renseignements personnels qui relèvent d'une institution fédérale ne peuvent être communiqués, à défaut du consentement de l'individu qu'ils concernent, que conformément au présent article.

(2) Sous réserve d'autres lois fédérales, la communication des renseignements personnels qui relèvent d'une institution fédérale est autorisée dans les cas suivants :

*a*) communication aux fins auxquelles ils ont été recueillis ou préparés par l'institution ou pour les usages qui sont compatibles avec ces fins ;

*b*) communication aux fins qui sont conformes avec les lois fédérales ou ceux de leurs règlements qui autorisent cette communication ;

*c*) communication exigée par *subpoena*, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de renseignements ;

*d*) communication au procureur général du Canada pour usage dans des poursuites judiciaires intéressant la Couronne du chef du Canada ou le gouvernement fédéral ;

*e*) communication à un organisme d'enquête déterminé par règlement et qui en fait la demande par écrit, en vue de faire respecter des lois fédérales ou provinciales ou pour la tenue d'enquêtes licites, pourvu que la demande précise les fins auxquelles les renseignements sont destinés et la nature des renseignements demandés ;

*f*) communication aux termes d'accords ou d'ententes conclus d'une part entre le gouvernement du Canada ou l'un de ses organismes et, d'autre part, le gouvernement d'une province ou d'un État étranger, une organisation internationale d'États ou de gouvernements, le conseil de la première nation de Westbank, le conseil de la première nation participante — au sens du paragraphe 2(1) de la *Loi sur la compétence des premières nations en matière d'éducation en Colombie-Britannique* — ou l'un de leurs organismes, en vue de l'application des lois ou pour la tenue d'enquêtes licites ;

*g*) communication à un parlementaire fédéral en vue d'aider l'individu concerné par les renseignements à résoudre un problème ;

*h*) communication pour vérification interne au personnel de l'institution ou pour vérification comptable au bureau du contrôleur général ou à toute personne ou tout organisme déterminé par règlement ;

*i*) communication à Bibliothèque et Archives du Canada pour dépôt ;

*j*) communication à toute personne ou à tout organisme, pour des travaux de recherche ou de statistique, pourvu que soient réalisées les deux conditions suivantes :

(i) le responsable de l'institution est convaincu que les fins auxquelles les renseignements sont communiqués ne peuvent être normalement atteintes que si les renseignements sont donnés sous une forme qui permette d'identifier l'individu qu'ils concernent,

d’une institution fédérale ne peuvent être communiqués, à défaut du consentement de l’individu qu’ils concernent, que conformément à cet article 8 (paragraphe 8(1)).

---

(ii) la personne ou l’organisme s’engagent par écrit auprès du responsable de l’institution à s’abstenir de toute communication ultérieure des renseignements tant que leur forme risque vraisemblablement de permettre l’identification de l’individu qu’ils concernent ;

*k*) communication à tout gouvernement autochtone, association d’autochtones, bande d’Indiens, institution fédérale ou subdivision de celle-ci, ou à leur représentant, en vue de l’établissement des droits des peuples autochtones ou du règlement de leurs griefs ;

*l*) communication à toute institution fédérale en vue de joindre un débiteur ou un créancier de Sa Majesté du chef du Canada et de recouvrer ou d’acquitter la créance ;

*m*) communication à toute autre fin dans les cas où, de l’avis du responsable de l’institution :

(i) des raisons d’intérêt public justifieraient nettement une éventuelle violation de la vie privée,

(ii) l’individu concerné en tirerait un avantage certain.

(3) Sous réserve des autres lois fédérales, les renseignements personnels qui relèvent de Bibliothèque et Archives du Canada et qui y ont été versés pour dépôt ou à des fins historiques par une institution fédérale peuvent être communiqués conformément aux règlements pour des travaux de recherche ou de statistique.

(4) Le responsable d’une institution fédérale conserve, pendant la période prévue par les règlements, une copie des demandes reçues par l’institution en vertu de l’alinéa (2)*e*) ainsi qu’une mention des renseignements communiqués et, sur demande, met cette copie et cette mention à la disposition du Commissaire à la protection de la vie privée.

(5) Dans le cas prévu à l’alinéa (2)*m*), le responsable de l’institution fédérale concernée donne un préavis écrit de la communication des renseignements personnels au Commissaire à la protection de la vie privée si les circonstances le justifient; sinon, il en avise par écrit le Commissaire immédiatement après la communication. La décision de mettre au courant l’individu concerné est laissée à l’appréciation du Commissaire.

(6) L’expression « bande d’Indiens » à l’alinéa (2)*k*) désigne :

*a*) soit une bande au sens de la *Loi sur les Indiens* ;

*b*) soit une bande au sens de la *Loi sur les Cris et les Naskapis du Québec*, chapitre 18 des Statuts du Canada de 1984 ;

*c*) soit la bande au sens de la *Loi sur l’autonomie gouvernementale de la bande indienne sechelte*, chapitre 27 des Statuts du Canada de 1986 ;

*d*) la première nation dont le nom figure à l’annexe II de la *Loi sur l’autonomie gouvernementale des premières nations du Yukon*.

(7) L’expression « gouvernement autochtone » à l’alinéa (2)*k*) s’entend :

*a*) du gouvernement nisga’a, au sens de l’Accord définitif nisga’a mis en vigueur par la *Loi sur l’Accord définitif nisga’a* ;

*b*) du conseil de la première nation de Westbank ;

*c*) du gouvernement tlicho, au sens de l’article 2 de la *Loi sur les revendications territoriales et l’autonomie gouvernementale du peuple tlicho* ;

*d*) du gouvernement nunatsiavut, au sens de l’article 2 de la *Loi sur l’Accord sur les revendications territoriales des Inuit du Labrador* ;

*e*) du conseil de la première nation participante, au sens du paragraphe 2(1) de la *Loi sur la compétence des premières nations en matière d’éducation en Colombie-Britannique* ;

*f*) du gouvernement tsawwassen, au sens du paragraphe 2(2) de la *Loi sur l’accord définitif concernant la Première Nation de Tsawwassen*.

(8) L'expression « conseil de la première nation de Westbank » aux alinéas (2)*f*) et (7)*b*) s'entend du conseil au sens de l'Accord d'autonomie gouvernementale de la première nation de Westbank mis en vigueur par la *Loi sur l'autonomie gouvernementale de la première nation de Westbank*.

Nous constatons que le législateur canadien a voulu établir le « principe de la limitation de l'utilisation » des renseignements personnels.

Ainsi, ce principe préconise que les renseignements personnels ne soient pas communiqués à autrui, ni utilisés à des fins autres que celles qui ont été spécifiées au moment de la collecte, sauf si la personne concernée a pu manifester son consentement ou si une règle de droit le permet.

Ce principe « se décompose essentiellement en trois éléments : la confidentialité des données, la non-communication des données à autrui et ce, même pour des fins compatibles, et finalement la non-utilisation des données recueillies contraire aux finalités initiales»[335]. Toutefois, ces restrictions ne peuvent pas être absolues, puisque « l'information, par nature, est appelée à circuler »[336].

Dès 1995, le CPVPC rendait public un rapport sur « Le dépistage génétique et la vie privée »[337], qui soulignait les faiblesses de la disposition régissant, dans la LPRP, la communication de renseignements personnels à caractère confidentiel :

> « Il est relativement facile pour une institution gouvernementale de révéler des renseignements personnels hautement confidentiels en vertu de l'alinéa 8(2). Cela continue à intéresser le bureau du Commissaire. Cet alinéa est une passoire. Ainsi par exemple, une institution gouvernementale peut accepter ou faire en sorte de révéler des renseignements personnels d'ordre génétique au gouvernement étranger ou à une organisation internationale d'État ou encore à toute institution ou organisation gouvernementale aux fins administratives de la loi. »[338]

Cette disposition, qui a été qualifié de « passoire », permet en effet de communiquer très facilement des renseignements personnels à des tiers, ce qui peut

---

[335] Karim BENYEKHLEF, préc., note 313, p. 120.
Le professeur Benyekhlef souligne que : « Le premier et deuxième éléments se confondent : le détenteur de données nominatives ne peut les communiquer à autrui. Le troisième élément du principe veut que les renseignements personnels puissent être communiqués à autrui si les finalités, en vue desquelles ils ont été collectés, sont les mêmes ou, à tout le moins, compatibles avec les nouvelles finalités ».

[336] *Id.*, p. 121.

[337] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Le dépistage génétique et la vie privée*, 1995.

[338] *Id*, p. 84 (nous soulignons).

poser des problèmes majeurs pour la maîtrise des renseignements personnels par les personnes concernées. Et cela, parce que les transferts peuvent se faire entre des gouvernements au Canada mais aussi en traversant les frontières nationales.

Ainsi, le paragraphe 8(2) renferme une série de cas où la communication de renseignements personnels relevant d'une institution fédérale est autorisée, sous réserve d'autres lois fédérales. Depuis le CPVPC, il est explicité que les exceptions de cette disposition viennent faire basculer l'équilibre posé par le consentement de la personne concernée :

> « Il faudrait enfin procéder à un examen minutieux des dispositions de la *Loi sur la protection des renseignements personnels* qui autorisent la communication sans consentement. La disposition sur la communication exige par défaut le consentement, mais les exceptions qui lui font suite sont larges au point d'ôter toute pertinence au critère de consentement original. »[339]

Le CPVPC considère que la LPRP ne traite pas adéquatement les obligations des institutions qui communiquent des renseignements personnels sans le consentement des personnes concernées. Ainsi, selon le CPVPC, l'institution devrait, dans la mesure du possible, obligatoirement informer la personne de la communication de ses informations, ce qui n'annulerait pas la possibilité de les communiquer si nécessaire, pouvant par un avis préalable contester la communication avant qu'elle ne soit effectuée[340].

Il s'agirait donc que la communication de renseignements personnels sans le consentement de la personne concernée ou sans préavis constitue une exception selon le paragraphe 8(2), plutôt qu'une option par défaut.

Il est recommandé que cette disposition fasse l'objet d'un examen approfondi permettant de déterminer dans quels cas un avis devrait absolument être donné

[339] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Reconstruire la Loi sur la protection des renseignements personnels*, Allocution présentée par Jennifer STODDART au Colloque organisé par Riley Information Systems, 21 février 2007, Ottawa.

[340] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 324, p. 30.

avant la communication et dans quels cas un avis pourrait être donné après la communication ainsi que les cas d'exception où il conviendrait de ne pas donner d'avis[341]. Bien sûr, dans le contexte de l'administration électronique, il est essentiel de se demander sous quelles conditions les organismes seront en mesure de communiquer des renseignements personnels et si les personnes concernées doivent donner leur avis pour certaines de ces communications d'informations.

Selon le CPVPC, les dispositions du paragraphe 8(2) manquent, de façon générale, de précision. Nous allons faire uniquement référence à celles qui peuvent avoir un intérêt pour ce qui est de la communication de renseignements personnels entre organismes publics et celles qui ont un impact sur la détermination des contours des usages compatibles et, en conséquence, du principe de finalité en droit fédéral canadien.

Il s'agira également de voir quelles dispositions du paragraphe 8(2) sont susceptibles d'être appliquées dans le contexte de l'administration en réseau ou de l'administration électronique.

L'alinéa 8(2)a) reprend le principe de « spécification des finalités » que le paragraphe 7(a) de la LPRP avait déjà énoncé[342], en autorisant la communication de renseignements personnels qui relèvent d'une institution fédérale dans le cas d'une « communication aux fins auxquelles ils ont été recueillis ou préparés par l'institution ou pour les usages qui sont compatibles avec ces fins »[343]. En effet, une communication des renseignements personnels sans le consentement de la personne concernée est possible si une telle communication se fait aux fins pour lesquelles l'institution les a obtenus ou pour un usage compatible avec ces fins.

Nous sommes ici face à la même problématique entourant l'article 7 de la LPRP : « C'est là une permission trop large : il vaudrait mieux appliquer le critère du "rapport raisonnable et direct" dans le cas d'un usage compatible »[344].

---

[341] *Id.*, p. 31.
[342] Voir à ce sujet : K. BENYEKHLEF, préc., note 313, p. 122.
[343] Nous soulignons.
[344] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 339.

Le CPVPC propose la modification de l'article 8 de la LPRP, afin de prévoir un « critère de lien raisonnable et direct » à appliquer à la communication des renseignements personnels, intégrant ainsi un élément voulant préciser quels usages compatibles justifient une telle communication[345].

Il est question ici d'identifier s'il existe un lien « raisonnable » et « direct » entre les usages qui motivent, d'une part, la collecte des renseignements et, d'autre part, la communication de ces renseignements. Le CPVPC considère que cette inclusion dans la LPRP peut contribuer à clarifier et restreindre les dispositions en matière de collecte et d'utilisation des renseignements personnels dans le secteur public canadien.

Sans aucun doute, l'ajout de ce critère aide à cerner le concept d'usage compatible que la rédaction actuelle de la loi nous fournit, mais cela ajoute aussi à cette problématique des défis intéressants.

Ainsi, nous aurons l'occasion d'étudier plus en profondeur dans les pages qui suivent quelle est la doctrine canadienne que nous pouvons dégager quant à la détermination des usages compatibles justifiant la communication de renseignements personnels et comment les critères proposés par le CPVPC pour encadrer cette question s'appliquent à l'exercice d'évaluation mentionné.

L'alinéa 8(2)b) va autoriser la communication aux fins qui sont conformes avec les lois fédérales ou ceux de leurs règlements qui autorisent cette communication. Nous pouvons identifier à première vue les problèmes posés par cette disposition, ce qui a provoqué le fait que le CPVPC préconise que les détails des communications apparaissent et soient définis dans la loi, au lieu de laisser la décision à la discrétion de l'institution[346].

Bien sûr, cette disposition laisse la porte ouverte à une multitude de communications d'informations entre les organisations du secteur public fédéral canadien à des fins que les lois et les règlements encadrent.

---

[345] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 324, p. 31.

[346] *Id.*

Nous observons également que d'autres lois fédérales canadiennes peuvent avoir pour effet de limiter ou d'étendre les dispositions qui encadrent la communication des renseignements personnels contenues dans la LPRP. Comme le CPVPC nous le rappelle, si une loi fédérale permet la communication de renseignements personnels dans des circonstances que la LPRP n'aurait pas permises, cette loi aurait préséance sur la LPRP s'il devait y avoir contradiction entre les deux[347].

Regardons également l'alinéa 8(2)m qui permet la communication à toute autre fin dans les cas où, de l'avis du responsable de l'institution :

a) des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée ;

b) l'individu concerné en tirerait un avantage certain[348].

Il convient attirer l'attention sur cette disposition qui laisse la porte ouverte à des transferts de renseignements personnels « à toute autre fin » pour des raisons « d'intérêt public » ou si la personne concernée en tire « un avantage certain ». Ainsi, le responsable de l'institution fédérale détentrice des informations est investi d'un grand pouvoir, tout à fait discrétionnaire, pour décider de ces transferts.

Comme certains l'ont précisé, le critère d'analyse fourni par cette disposition ne permet pas « en raison d'un laconisme inexplicable, au responsable d'évaluer avec justesse les situations où la communication des renseignements s'impose »[349]. Certains remarquent que rien dans le libellé de cette disposition ne vient conférer à l'exercice un semblant d'objectivité et de rationalité et ajoutent :

> « Le responsable se meut plutôt dans un univers constellé de notions aussi abstraites que l'intérêt public ou l'avantage certain. Aucun paramètre précis ne cible ou n'encadre son action. »[350]

Nous notons ici que cette disposition renferme une exception un peu trop généralisée et que, « à trop vouloir prévoir l'imprévisible, par le biais d'une

[347] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 337, p. 86.
[348] Nous soulignons.
[349] K. BENYEKHLEF, préc., note 313, p. 123.
[350] *Id.*

disposition résiduaire de la nature de l'alinéa m), le législateur nous semble avoir édulcoré le caractère fondamental du principe de non-communication »[351]. Nous sommes face à une situation laissant au responsable de l'institution la possibilité d'invoquer cette disposition afin d'avoir une très large marge de manœuvre à l'heure de communiquer des informations, ce qui risque de devenir un recours courant, au lieu de représenter une exception au régime général.

Le paragraphe 8(5) de la LPRP stipule que, dans le cas prévu dans l'alinéa 8(2)m), le responsable de l'institution fédérale détentrice des informations doit donner un préavis écrit de la communication des renseignements personnels au CPVPC si les circonstances le justifient et, sinon, doit en aviser le CPVPC après la communication. C'est au CPVPC de mettre au courant l'individu concerné s'il le juge nécessaire en pouvant intervenir et recommander que les renseignements ne soient pas communiqués. L'article 9[352], le sous-alinéa 11(1)a)iv) et le paragraphe 11(2)[353] de la LPRP prescrivent que toutes les fins pour lesquelles les

[351] *Id.*, p. 124.

[352] 9. (1) Le responsable d'une institution fédérale fait un relevé des cas d'usage, par son institution, de renseignements personnels versés dans un fichier de renseignements personnels, ainsi que des usages ou fins auxquels ils ont été communiqués par son institution si ceux-ci ne figurent pas parmi les usages et fins énumérés dans le répertoire prévu au paragraphe 11(1), en vertu du sous-alinéa 11(1)*a*)(iv) et du paragraphe 11(2); il joint le relevé aux renseignements personnels.

(2) Le paragraphe (1) ne s'applique pas aux renseignements communiqués en vertu de l'alinéa 8(2)*e*).

(3) Le relevé mentionné au paragraphe (1) devient lui-même un renseignement personnel qui fait partie des renseignements personnels utilisés ou communiqués.

(4) Dans les cas où des renseignements personnels versés dans un fichier de renseignements personnels relevant d'une institution fédérale sont destinés à un usage, ou communiqués pour un usage, compatible avec les fins auxquelles les renseignements ont été recueillis ou préparés par l'institution, mais que l'usage n'est pas l'un de ceux qui, en vertu du sous-alinéa 11(1)*a*)(iv), sont indiqués comme usages compatibles dans le répertoire visé au paragraphe 11(1), le responsable de l'institution fédérale est tenu :

*a*) d'aviser immédiatement le Commissaire à la protection de la vie privée de l'usage qui a été fait des renseignements ou pour lequel ils ont été communiqués ;

*b*) de faire insérer une mention de cet usage dans la liste des usages compatibles énumérés dans l'édition suivante du répertoire.

[353] 11.(1) Le ministre désigné fait publier, selon une périodicité au moins annuelle, un répertoire :

*a*) d'une part, de tous les fichiers de renseignements personnels, donnant, pour chaque fichier, les indications suivantes :

renseignements sont recueillis, les usages compatibles avec ces fins et toutes les communications de renseignements personnels soient enregistrés, justifiés et consignés s'il y a lieu dans un répertoire de renseignements personnels (*Info Source*) afin que les personnes concernées puissent connaître tout ce qui traite de la gestion de leurs renseignements personnels.

*Info Source* est « une série de publications annuelles du SCT dans lesquelles les institutions fédérales sont tenues de décrire leurs organisations, leurs responsabilités en matière de programmes et leurs fonds de renseignements, dont les fichiers de renseignements personnels et les catégories de renseignements personnels qu'elles détiennent »[354].

---

(i) sa désignation, son contenu, la cote qui lui a été attribuée par le ministre désigné, conformément à l'alinéa 71(1)*b*), ainsi que la désignation des catégories d'individus sur qui portent les renseignements personnels qui y sont versés,
(ii) le nom de l'institution fédérale de qui il relève,
(iii) les titre et adresse du fonctionnaire chargé de recevoir les demandes de communication des renseignements personnels qu'il contient,
(iv) l'énumération des fins auxquelles les renseignements personnels qui y sont versés ont été recueillis ou préparés de même que l'énumération des usages, compatibles avec ces fins, auxquels les renseignements sont destinés ou pour lesquels ils sont communiqués,
(v) l'énumération des critères qui s'appliquent à la conservation et au retrait des renseignements personnels qui y sont versés,
(vi) s'il y a lieu, le fait qu'il a fait l'objet d'un décret pris en vertu de l'article 18 et la mention de la disposition des articles 21 ou 22 sur laquelle s'appuie le décret ;
*b*) d'autre part, de toutes les catégories de renseignements personnels qui relèvent d'une institution fédérale mais ne sont pas versés dans des fichiers de renseignements personnels, donnant, pour chaque catégorie, les indications suivantes :
(i) son contenu, en termes suffisamment précis pour faciliter l'exercice du droit d'accès prévu par la présente loi,
(ii) les titre et adresse du fonctionnaire de l'institution chargé de recevoir les demandes de communication des renseignements personnels qu'elle contient.

(2) Le ministre désigné peut insérer, dans le répertoire, des usages ou fins non prévus au sous-alinéa (1)*a*) (iv) mais s'appliquant, dans le cadre de communications courantes, à des renseignements personnels versés dans les fichiers de renseignements personnels.

(3) Le ministre désigné est responsable de la diffusion du répertoire dans tout le Canada, étant entendu que toute personne a le droit d'en prendre normalement connaissance.

[354] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 325.
Le SCT ajoute ces idées quant au contenu d'*Info Source* :
« Les renseignements doivent être suffisamment clairs et détaillés, pour permettre au public d'exercer son droit d'accès en vertu de la Loi sur la protection des renseignements personnels. Les activités de couplage de données, l'utilisation du NAS et toutes les activités pour lesquelles des évaluations des facteurs relatifs à la vie privée ont été effectués doivent être mentionnés dans les FRP d'Info Source, le cas échéant. Les publications Info Source présentent également les coordonnées des ministères et organismes fédéraux ainsi que des résumés des causes de la Cour fédérale et des statistiques sur les demandes d'accès. ».

Ainsi, cette obligation d'énumérer les fins premières et les fins compatibles avec celles-ci est à la base de l'obligation de rendre compte des usages et des communications qui dérive des articles 7 et 8 de la LPRP et constitue « un des principaux moyens dont dispose le gouvernement pour aviser le public de la façon dont il va utiliser les renseignements personnels »[355].

Cependant, le paragraphe 11(2) a voulu encadrer une catégorie qui n'entre pas dans les catégories de « fins de collecte » ou « d'usage compatible », en autorisant le ministre désigné à inclure dans la description des fichiers de renseignements personnels les énoncés des « usages courants » des renseignements, comme dans les cas de communications de renseignements personnels en vertu du paragraphe 8(2) de la LPRPD qui se produisent sur une base régulière.

Les paragraphes 9(1) et 9(3) visent à faire en sorte que la personne concernée puisse savoir quels usages sont faits des renseignements les concernant qui ne figurent pas dans *Info Source*. Étant donné que le relevé des usages et communications est joint aux renseignements personnels, il sera accessible au même titre que les renseignements et facilitera l'étude des cas d'usage et de communication par le CPVPC[356].

Le paragraphe 9(4) encadre les cas exceptionnels où une institution va devoir utiliser ou communiquer des renseignements à des fins qui, tout en étant compatibles avec les fins pour lesquelles ils ont été obtenus ou consignés, n'étaient pas prévues et ne figuraient pas dans *Info Source*. Nous constatons que la LPRP fournit des mécanismes permettant une certaine transparence dans la gestion des renseignements personnels, afin que les personnes concernées puissent connaître les usages et les communications ayant pour objet leurs renseignements personnels.

Il faut également noter qu'en vertu de l'article 73 de la LPRP, le responsable de l'institution fédérale détentrice des informations détient un pouvoir qui va lui

---

[355] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 332.

[356] Voir à ce sujet : *Id.*
Il faut noter que ces relevés vont devoir être conservés pendant au moins deux ans après l'usage ou la communication.

permettre, par arrêté, de déléguer certaines de ses attributions à des cadres ou employés de l'institution.

En 1995, le CPVPC a recommandé, pour ce qui est des renseignements de nature génétique, que, dans les cas où des renseignements personnels relevant d'institutions fédérales constituent des « usages compatibles », le responsable de l'institution est celui qui doit, dans tous les cas, approuver les utilisations qui en sont faites. Il a souhaité également que, comme politique, cette décision ne devrait jamais faire l'objet d'une délégation[357].
Le CPVPC souligne également que, de façon générale, il faudrait obtenir également le consentement personnel du responsable de l'institution dans les cas prévus à l'alinéa 8(2)a), quand il s'agit de communications pour des usages compatibles avec les fins pour lesquelles les renseignements ont été recueillis ou préparés par l'institution.

Même si ces recommandations ont été faites dans le contexte d'une étude de la protection des renseignements personnels de nature génétique, nous considérons qu'elles sont tout à fait applicables à toutes les données si elles sont de nature sensible ou si les communications peuvent donner lieu à un risque en matière de protection de la vie privée des personnes concernées.
Il faut noter que, actuellement, le SCT a établi une liste des cas où le pouvoir du responsable peut être délégué. Nous retrouvons dans cette liste fermée adressée aux personnes travaillant dans les organismes publics fédéraux deux des cas prévus au paragraphe 8(2) : les cas de communication à des fins de recherche (alinéa 8(2)j)) et le cas de communication dans l'intérêt public ou d'une personne (alinéa 8(2)m)).

Pour le contrôle d'application des articles 4 à 8 de la LPRP, le CPVPC va pouvoir, à son appréciation, mener des enquêtes sur les renseignements relevant des institutions fédérales (paragraphe 37(1)). S'il considère, à l'issue de son enquête,

[357] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 337, p. 83.

qu'un organisme n'a pas appliqué ces dispositions, il va pouvoir adresser aux responsables de l'institution un rapport où il présente ses conclusions ainsi que les recommandations qu'il juge indiquées (paragraphe 37(3)).
Les citoyens ont également la possibilité de présenter une plainte devant le CPVP, pouvant procéder à une enquête sur des questions relatives à la collecte, la conservation ou le retrait par une institution fédérale des renseignements personnels ou sur l'usage ou la communication des renseignements relevant des organismes publics fédéraux ( alinéa 29(1) (h) i) ii)).

Il faut noter également que les responsables des institutions fédérales sont tenus de présenter au Parlement un rapport d'application de la LPRP en ce qui concerne son institution[358]. Toutefois, il serait souhaitable de renforcer les obligations contenues dans cette disposition afin d'obliger les institutions à rendre compte au Parlement d'un plus large éventail de pratiques, en intégrant à la LPRP les exigences législatives des Lignes directrices en la matière prévues par le SCT[359]. En effet, le CST a publié en 2005 des lignes directrices au sujet des rapports concernant la protection des renseignements personnels, qui ont été mises à jour en 2008. Cet instrument spécifie que les institutions doivent présenter dans le rapport annuel une indication du nombre de nouvelles activités de couplage et d'échange de données avec d'autres institutions qui ont été entreprises dans l'année, ainsi que les activités internes dans les divers services de l'institution. Nous observons que cette obligation devrait être prévue dans la LPRP afin d'assurer un minimum de transparence sur les échanges et communications de données au sein du secteur public canadien.

[358] Paragraphe 72(1) de la LPRP.
[359] SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Rapports annuels sur la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels - Rapport de mise en œuvre n 109*, en ligne : http://www.tbs-sct.gc.ca/atip-aiprp/impl-rep/2008/109-imp-mise-fra.asp (consulté le 3 décembre 2010).

**D - Secteur privé canadien**

Nous avons pu analyser dans les pages précédentes la façon dont la LPRPDE encadre la protection des renseignements personnels dans le secteur privé canadien. Il sera question dans les prochaines pages d'examiner brièvement comment la LPRPDE a abordé la question de la finalité des renseignements personnels dans le contexte du secteur privé, afin d'analyser le droit canadien dans ce contexte, même si *a priori* les dispositions de cette loi ne sont pas d'application dans le cadre de l'administration publique ni du gouvernement électronique.

Le paragraphe 5.1 de la LPRPDE établit que « sous réserve des articles 6 à 9, toute organisation doit se conformer aux obligations énoncées dans l'annexe 1 », ce qui montre effectivement que les principes contenus dans cette annexe 1 se traduisent par l'établissement de conditions minimales en ce qui concerne la protection des renseignements personnels dans le secteur privé canadien.

Nous étudierons les dispositions faisant référence au principe de finalité dans la LPRPDE, une loi qui a voulu répondre aux déficiences de la LPRP relative au secteur public, par le biais de l'introduction de nouveaux éléments. Ainsi, nous observerons un passage de « l'usage compatible » présent dans la LPRP aux « fins acceptables » que la LPRPDE a introduit pour le secteur privé fédéral canadien.

Le législateur canadien a répondu de cette façon aux voix qui demandaient l'introduction d'éléments aidant à déterminer la légitimité d'utilisation des renseignements personnels.

Nous analyserons ces dispositions afin de comprendre quel a été le passage d'un modèle à l'autre dans la gestion de cette question, même si la LPRPDE ne s'applique pas au secteur public canadien ni au réseau de l'administration électronique. Nous aurons l'occasion de constater que certaines des recommandations suggérant la réforme de la LPRP trouvent un écho dans la nouvelle rédaction de la LPRPDE.

Nous remarquons que la LPRPDE démontre, dans la détermination des « fins » de la collecte, l'importance de l'utilisation et de la communication des renseignements personnels. Ce texte souligne également la portée de cet objectif, qui se trouve au cœur du texte, et relie ce concept à ceux de la « raisonnabilité » et de « l'acceptable dans les circonstances » :

> « (...) de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. »[360]

Voici l'esprit de la LPRPDE qui a introduit dans le droit canadien relatif à la protection des renseignements personnels les critères de ce qu'une personne « raisonnable », estimerait « acceptable », mais en conditionnant cela aux « circonstances ». C'est ce schéma qui donne de nouveaux outils pour interpréter et déterminer les fins auxquelles les renseignements peuvent servir.

Ainsi, la LPRPDE encadre les « fins acceptables » en notifiant que « l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptable dans les circonstances »[361].

Nous pouvons nous demander quel sens donner à ces trois expressions, utilisées conjointement dans cette disposition, afin de déterminer la légitimité des fins auxquelles les renseignements sont recueillis, utilisés ou communiqués. Notons également que ces trois actions sont jugées équivalentes, pour ce qui est des risques de vulnérabilisation du droit à la protection des renseignements personnels en cas de non-respect de cette disposition.

---

[360] Article 3 LPRPDE (nous soulignons).
[361] Paragraphe 5(3) de la LPRPDE (nous soulignons).

Voici le « Critère de la personne raisonnable », comme le CPVPC l'a désigné, qui va imposer d'importantes contraintes aux organisations et qui va les empêcher d'énoncer en des termes trop larges ou vagues les fins pour lesquelles les renseignements ont été recueillis[362].

L'article 7 encadre la collecte (paragraphe 7(1)), l'utilisation (paragraphe 7(2)) et la communication (paragraphe 7(3)) à l'insu de l'intéressé et sans son consentement en fournissant une liste fermée des cas permettant ces opérations sans le consentement de la personne concernée.

Cette disposition comprend des exceptions au principe général que la LPRPDE impose et tient compte des dérogations à la règle générale afin de limiter la collecte, l'utilisation et le transfert de renseignements personnels.

Nous aurons l'occasion d'étudier dans les pages qui suivent comment ce critère de la personne raisonnable a fait évoluer le concept des « fins acceptables » dans le droit fédéral canadien et comment ces concepts ont influencé la définition des contours de la notion des « fins d'utilisation » dans le secteur public et privé.

**2 - Les principes dans les textes**

L'étude du principe de finalité de façon isolée ne permet pas d'avoir un véritable aperçu du système de protection basé sur l'ensemble des principes de protection. De plus, les différents principes appellent à une application qui tienne compte du reste. Une vision d'ensemble s'impose afin de comprendre comment les textes encadrent la protection des renseignements personnels.

Nous avons étudié comment les textes œuvrant dans le contexte européen établissent de façon très claire les principes de loyauté de la collecte et du traitement, ainsi que le principe de spécification des finalités.

[362] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2000-2001*, 2001.

Nous observons dans le paysage canadien que le principe de détermination des fins de la collecte a été adopté dans le contexte du secteur privé (paragraphe 4(2) Annexe 1 de la LPRPDE)) et que d'autres textes parlent plutôt des usages des renseignements personnels au sein de l'administration (Article 7 de la LPRP).

Le cadre légal canadien se base fondamentalement sur les principes relatifs à la limitation de l'utilisation, de la communication et de la conservation des renseignements personnels (paragraphe 4(5) Annexe 1 de la LPRPDE ), ainsi que sur des règles trouvant leur base dans les conditions devant régir la collecte des renseignements personnels, la conservation et le retrait de ces renseignements personnels dans le contexte du secteur public (Articles 4 à 6 de la LPRP).

Nous retrouvons également dans le contexte canadien des règles régentant la communication des renseignements personnels (Article 8 de la LPRP) dans l'administration et d'autres préconisant le principe d'exactitude (paragraphe 4(6) Annexe 1 de la LPRPDE)) des renseignements détenus par les organisations appartenant au secteur privé.
Le principe relatif à la qualité des données est également présent dans les dispositions contenues dans les instruments canadiens et européens (par exemple, à l'article 5 de la Convention 108 et au paragraphe 6(3) de la Loi et L modifiée). Un principe sur les conditions de conservation des données sous forme nominative par rapport aux finalités de collecte et de traitement (paragraphe 6(5) de la Loi I et L) est également préconisé par les textes.

Le catalogue de dispositions se divise parfois très clairement en « Obligations incombant aux responsables de traitements et droits des personnes » (Chapitre V de la Loi I et L) et en « Droits des personnes à l'égard des traitements de données à caractère personnel » (Section II de la Loi I et L modifiée) en reprenant ainsi les principes basiques de protection contenus également dans la Convention 108 et dans la Directive 95/46/CE.

Nous identifions ainsi certains droits des personnes à l'égard des traitements de données à caractère personnel, droits pouvant être exercés par les titulaires des renseignements personnels, tels que le droit d'accès de la personne concernée à ses données (par exemple, à l'article 12 de la Directive 95/46/CE et au paragraphe 4(9) Annexe 1 de la LPRPDE), le droit d'opposition de la personne concernée à que ses données soient traitées (article 14 de la Directive 95/46/CE et arts. 38 et suiv. de la Loi I et L modifiée), ainsi que le droit de rectification.
Nous repérons également le principe de « l'information de la personne concernée » (par exemple, aux articles 10 et 11 de la Directive 95/46/CE et article 32 de la Loi I et L modifiée) ainsi que d'autres dispositions consacrant le principe de transparence (paragraphe 4(8) Annexe 1 de la LPRPDE) devant être respecté dans le contexte des traitements à caractère personnel.

Les textes accordent également une importance particulière aux « Décisions individuelles automatisées » (article 15 de la Directive 95/46/CE), en reconnaissant le droit à toute personne de ne pas être soumise à une décision prise sur le seul fondement d'un traitement automatisé de données.

Nous observons que les textes disposent quelles sont les « Obligations incombant aux responsables de traitements » (Section 1 de la Loi I et L modifiée) et affirment le principe de responsabilité (paragraphe 4(1) Annexe 1 de la LPRPDE)), le principe relatif aux garanties complémentaires pour la personne concernée (art.8 de la Convention 108), ainsi que les principes de confidentialité (article 16 de la Directive 95/46/CE) et de sécurité des traitements (article 17 de la Directive 95/46/CE, article 7 de la de la Convention 108 et article 34 de la Loi I et L modifiée et art. 4.7 Annexe 1 de la LPRPDE).

Les législateurs ont procédé à la catégorisation de certaines données comme étant « sensibles » (article 8 de la Directive 95/46/CE) et pose les conditions pour établir des traitements portant sur des « Catégories particulières de traitements » (article 6

de la Convention 108 et articles 8 à 10 de la Loi I et L modifiée), qui visent à leur accorder une protection particulière en raison de leur degré de sensibilité.

Nous notons également que les textes établissent les conditions à respecter lors des transferts de données à caractère personnel vers des pays tiers (par exemple, aux articles 25 et 26 de la Directive 95/46/CE et aux arts. 68 et suiv. de la Loi I et L modifiée).

Des questions relatives aux exceptions et restrictions (art. 9 de la Convention 108), aux sanctions et aux recours (art. 10 de la Convention 108) ainsi qu'à la présentation d'une plainte (paragraphe 4(10) Annexe 1 de la LPRPDE) ont également été abordées par les textes en la matière.

Certaines dispositions font référence au principe du consentement (article 7 de la Loi I et L modifiée et paragraphe 4(3) Annexe 1 de la LPRPDE) de la personne concernée comme règle générale et condition essentielle pour le traitement de ses renseignements personnels.

En effet, une des nouveautés découlant de la Loi I et L modifiée est celle qui fait référence à la consécration à titre de principe général, de l'obligation d'obtenir le consentement des personnes fichées pour la mise en œuvre des traitements.
Comme certains l'ont souligné, le législateur a profité de la réforme de la loi française pour ériger le consentement à titre de principe à l'article 7 de la Loi I et L modifiée. Nous observons la grande importance que le législateur accorde à la nécessité du consentement, même si ce principe n'existait pas dans l'ancienne loi[363].

Toutefois, le législateur a également multiplié considérablement le régime des exceptions, « au point qu'on peut se demander si les exceptions ne sont pas

[363] Voir à ce propos : A. LEPAGE, préc., note 69, p. 234.

devenues la règle »[364]. Il faut mettre l'accent sur une des cinq conditions pouvant remplacer à l'exigence du consentement que la loi I et L modifiée prévoit.

En effet, nous pouvons citer comme exemple l'exécution d'une mission de service public comme étant une des exceptions à la règle générale de l'obtention du consentement pour la mise en œuvre d'un traitement. Il s'agit de voir si la mise en place des fonctionnalités et des services propres à l'administration électronique pourrait s'assimiler à une mission de service public, pouvant supposer une exception au régime général du consentement préalable. Tout cela, bien sûr, si des conditions existent pour que les données personnelles restent confidentielles.

En général, nous retrouvons un catalogue de principes de protection des renseignements personnels plus ou moins équivalent, et cela des deux côtés de l'Atlantique. Le principe de finalité doit être appliqué au regard de cet ensemble de principes formant un « tout » qui accorde aux renseignements personnels une protection de base.

[364] A. SENDRA, préc., note 244, p. 201.

**PARTIE 1 : L'application du principe de finalité et le recours aux standards en matière de protection des renseignements personnels**

## CHAPITRE 1 INTERPRÉTATION DU PRINCIPE DE FINALITÉ

Nous analyserons des documents de différentes natures, notamment les rapports annuels produits par les autorités de contrôle, afin de décrypter comment le critère de la finalité a été interprété dans le passé. Ces rapports sont une source importante de doctrine, puisqu'ils reprennent pour chaque année les avis, les délibérations, les dossiers et les contrôles les plus significatifs dans le cas de la CNIL et du CPVPC.

### SECTION 1 La doctrine dans le contexte français : les fondements du principe de finalité

La CNIL a élaboré une doctrine sur le principe de finalité que nous retrouvons dans les rapports annuels et qui constitue probablement la source d'information sur l'application de ce principe la plus complète à examiner.
L'examen de cette doctrine va nous permettre de dresser une synthèse, tout en faisant ressortir les lignes directrices résultant des avis et délibérations que la CNIL a élaborées au cours des années et qui peuvent présenter un intérêt pour le sujet qui nous occupe.

Dès le Rapport où la CNIL présente son « Bilan et perspectives » pour les années 1978-1980, le principe de finalité occupe clairement une place de grande importance : « L'adéquation des données enregistrées à la finalité du traitement est une idée directrice plus féconde que les interdictions à priori »[365]. Par conséquent, la CNIL entend être en mesure d'apprécier, par rapport à la finalité énoncée, la

[365] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Rapport de la Commission Nationale de l'Informatique et des Libertés, Bilan et perspectives, 1978-1980*, Paris, La Documentation Française, 1980, p. 27.

pertinence des informations collectées, de leur communication et de leurs programmes[366].

La CNIL signale que c'est grâce à la combinaison des dispositions faisant référence à la finalité présentes dans la législation française en la matière, aux dispositions du Code Pénal français réprimant le détournement de finalité et à l'article 5 de la Convention 108, qu'elle a développé son contrôle sur la finalité des traitements et qu'elle apprécie couramment si les informations à traiter sont non pertinentes et non excessives au regard de la finalité des traitements[367].

La CNIL souligne à nouveau cette idée en 1996 : « C'est plus certainement dans le registre juridique de la finalité, finalité qui devrait être très encadrée, et dans le champ de la sanction qui s'attache au détournement de la finalité, que se trouvent ici les garanties les plus adéquates »[368].

**1- Une notion à contours indéfinis**

La notion de finalité présente une certaine complexité, qui se multiplie encore si nous étudions l'ensemble des notions qui ont été apportées par la doctrine dans les dernières années.

Par finalité d'un traitement automatisé, il faut entendre son « objet », son « objectif précis» ou bien « l'objectif principal d'une application informatique de données personnelles »[369].

Dans son 2e Rapport, la CNIL fait référence à des concepts dont elle s'est servie à l'heure de rédiger ses délibérations et qui nous servent à comprendre la complexité du principe de finalité. Ainsi, la CNIL introduit des concepts clés qui ne se trouvent pas dans la Loi I et L et qui servent à nourrir notamment ce concept de finalité. De cette façon, la CNIL constate que, dans le cadre de la création d'un traitement, le

[366] *Id.*
[367] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 41, p. 64.
[368] *Id.*
[369] Cette définition est celle qui est accordée à la notion de « Finalité d'un traitement » dans le « Lexique Informatique et Libertés » que la CNIL publie chaque année dans ses Rapports Annuels.

système projeté comporte une « finalité principale », ainsi que des « finalités secondaires »[370].

De la même façon, dans une autre Délibération de 1981[371], la CNIL note que le recensement a, dans son cas, une « double finalité », sauf que seule la réalisation de la deuxième finalité donne lieu à des traitements automatiques d'informations.

La CNIL parle de « finalité principale »[372] à l'occasion de l'examen du système GAMIN[373], en procédant à la redéfinition les finalités d'un tel système, ce qui a permis l'évaluation et le contrôle de l'adéquation du système aux finalités poursuivies[374].

Il est également intéressant de voir que, pour certains traitements, la CNIL détermine pour « seules finalités » une liste plutôt fermée, avant de plus tard parler d'une « finalité principale », en introduisant d'une certaine manière le critère de hiérarchie parmi ces finalités[375].

Nous constatons que la doctrine de la CNIL a très clairement établi, depuis 1982, que tout traitement automatisé d'informations nominatives doit correspondre à une ou plusieurs finalités, qui vont devoir être indiquées lors des formalités préalables à

---

370 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *2e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1981, p. 209.
La CNIL constate cela dans ce document :
COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n° 81-07 du 3 février 1981 portant avis relatif à la création d'un traitement automatisé d'informations nominatives concernant les titres de séjour des étrangers.*
Dans cette Délibération, la CNIL établit que « le titre de séjour ne doit pas pouvoir être détourné de sa finalité, et qu'en particulier, il ne doit pas pouvoir être utilisé comme clé d'accès automatique à des systèmes d'informations automatisées ».

371 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération nº 81-03 du 10 mars 1981 portant avis relatif à la création de traitements automatisés d'informations nominatives effectués sur la base des informations collectées à l'occasion du recensement général de la population de 1982.*

372 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération nº 81-74 du 16 juin 1981 portant décision et avis relatifs à un traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile.*

373 Gestion automatisée de médecine infantile.

374 C'est à cette occasion que la CNIL détermine dans le cadre de ce traitement, que dans sa « finalité principale » le système se révèle soit contestable, soit inutile ou inutilisé.

375 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération nº 81-88 du 21 juillet 1981 portant avis sur la mise en œuvre d'un traitement automatisé du répertoire national des entreprises et établissements (SIRENE).*

sa mise en œuvre[376]. La CNIL établit très clairement que « la définition de la finalité doit être suffisamment précise pour couvrir toutes les applications, mais elle ne doit pas être trop large ni formulée d'une manière ambigüe ou équivoque »[377]. Sans oublier qu'une déclaration complémentaire doit être faite lorsqu'une modification de la finalité paraît nécessaire.

La CNIL nous rappelle qu'elle a été obligée d'examiner la notion de finalité aussi bien dans les dossiers de demande d'avis qui lui ont été soumis que lors de l'élaboration de normes simplifiées[378] et précise que le principe de finalité est une des bases des différentes normes simplifiées[379].

Nous constatons également, lors de l'examen des rapports annuels de la CNIL, que, au fil des années, les détournements de finalité ont été identifiés normalement suite à la présentation d'une série de plaintes déposées auprès de la CNIL, posant certains problèmes et se répétant dans le temps[380]. Toutefois, l'utilisation des fichiers publics et privés de gestion en période électorale a été à l'origine de nombreux détournements de finalité, pouvant faire l'objet de sanctions pénales, ce qui a motivé le fait que la CNIL définisse une déontologie en 1985[381].
Il faut noter que, dans les cas les plus graves d'utilisation à des fins de propagande politique et électorale, l'autorité française a dû envoyer des avertissements

[376]COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 370, p. 80.
[377] *Id*.
[378] *Id*.
[379] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Dix ans d'informatique et libertés*, Paris, Economica, 1988, p. 37.
[380] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *6e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1985, p. 53 et s.
Nous constatons que le problème général est notamment celui des cessions commerciales de fichiers mais également l'extension de finalité non-déclarée ou l'utilisation de fichiers par des tiers non autorisés.
[381] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n° 85-60 du 5 novembre 1985 portant recommandation relative à l'utilisation par les candidats aux élections politiques et les partis politiques de fichiers publics et privés, en vue de l'envoi de documents de propagande et de la recherche de financement*.

solennels[382]. La CNIL, qui a été fréquemment saisie de plaintes à propos de l'envoi, par les partis politiques et les candidats aux élections, de propagande et de demandes de financement, et cela à partir de l'utilisation non autorisée des fichiers de gestion, a voulu définir les cas dans lesquels cette utilisation était régulière.

De cette Recommandation nous pouvons faire ressortir deux points essentiels : d'une part, que le principe de finalité amène à proscrire l'utilisation directe ou indirecte de différents fichiers, tels que les fichiers informatisés fiscaux et certains répertoires comme les banques de données économiques et le fichier Sirène[383] ; d'autre part, certains fichiers comme les fichiers commerciaux, les listes électorales en période électorale et l'annuaire téléphonique, peuvent être utilisés moyennant certaines conditions, par contre d'autres fichiers comme ceux des anciens élèves des grandes écoles, ne peuvent pas être utilisés dans un tel contexte.
Cette doctrine de la CNIL a contribué à limiter les usages de certains fichiers afin de respecter le principe de finalité, notamment en période électorale, grâce à la définition d'une déontologie *ad hoc*.

Nous observons que, dans le passé, le législateur français a soumis les traitements du secteur public à un régime d'autorisation en lieu et place du régime qui comporte une simple déclaration, et cela parce l'Administration dispose d'un éventail de prérogatives considérables face aux citoyens. La CNIL, dans ce cas, fait jouer une procédure d'avis tacite, même si elle arrive à influer sur les choix d'informatisation qu'elle examine[384].
En raison de leur caractère exemplaire, certains projets de traitements ont donné lieu à la création d'un rapport assorti d'une délibération. En effet, les questions entourant la finalité du traitement ont motivé un examen particulier en raison de deux critères.

---

[382]COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 379, p. 38.
[383] Sirène est une base de données des entreprises et des établissements.
[384] COMMISION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *4e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1983, p. 40.

D'une part, il est question de la nature et l'importance de la population concernée par le traitement et, d'autre part, des problèmes de principe soulevés, concernant notamment les fichiers à « finalités multiples » et les traitements expérimentaux conçus en systèmes de réseaux[385].

C'est en effet les traitements du secteur public comportant plusieurs finalités et de multiples usages et pouvant être reliés ou interconnectés qui ont été examinés par la CNIL plus profondément et de façon plus détaillée.
L'existence de la procédure des normes simplifiées[386] afin de rendre possible l'existence d'une procédure allégée face à la procédure de droit commun a été critiquée dans le passé. En effet, certains ont souligné le caractère trop rigide des normes simplifiées qui peut conduire « au conformisme informatique et empêcheraient de d'envisager des choix novateurs »[387], concernant notamment les fichiers à « finalités complémentaires ».

La plus grande difficulté, à l'heure d'appliquer cette procédure allégée, se trouve également reliée aux questions complexes entourant une finalité qui n'est pas unitaire mais qui peut avoir des finalités complémentaires, puisque la rigidité d'une telle procédure tire son origine d'une vision plutôt « statique » de la finalité du traitement.

Il faut noter également la complexité et la richesse de la doctrine que la CNIL a élaborée au fil des années sur le concept de finalité, qui nous apporte des figures telles que les « finalités multiples » et les « finalités complémentaires », toutes deux particulièrement intéressantes et présentes dans le 4e Rapport d'activité. Notons que la CNIL a reconnu le cas des traitements à finalités multiples, par le biais d'un avis très novateur au regard du principe de finalité, en reconnaissant la possibilité de finalités multiples en l'encadrant précisément.

---

[385] *Id.*
[386] Procédure prévue à l'article 17 de la Loi I et L, afin d'alléger au maximum les formalités à accomplir pour la mise en œuvre des traitements.
[387] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 384, p. 42.

À cette occasion, la CNIL a consacré la « dualité des finalités » du fichier admettant qu'il puisse être exploité à la fois pour les besoins de l'administration et pour la satisfaction des intérêts de l'industrie[388].
Cet avis est le reflet du souci de la CNIL de ne pas s'en tenir à un « critère purement organique qui l'aurait conduite à n'admettre que des modes de gestion uniformes des fichiers »[389]. Certains affirment que cette répartition n'est plus adaptée, puisque la dangerosité pour les libertés ne dépend pas tant de la nature publique ou privée des responsables du traitement « mais des caractéristiques des données recueillies et de la finalité du traitement »[390]. En tout cas, ce qui montre la différence de régime établi par le législateur de 1978 est plutôt la crainte relative aux données détenues par les organismes publics.

Pour certains, l'application du principe de finalité requiert une certaine « souplesse » puisqu'elle est une notion « évolutive », ce qui devient évident lorsqu'elle est adoptée par la CNIL, l'expression faisant alors référence aux « finalités multiples ». Selon cette hypothèse, les finalités multiples ont été conçues dès l'origine et ont été déclarées comme telles à l'appui de formalités préalables auprès de la CNIL.
La CNIL affirme depuis des années que les finalités doivent être détaillées et énumérées et que, dans les cas ou elle autoriserait des « finalités multiples », elles doivent être très nettement distinguées et précisées.

Cette souplesse que requiert l'application du principe de finalité est évidente lorsqu'on étudie la manière d'établir une définition *a priori* des finalités à l'heure de respecter les formalités préalables à la création d'un traitement. Par ailleurs, pour certains programmes comportant des traitements de données personnelles, selon des

---

[388] Voir à ce sujet : C. MARLIAC-NÉGRIER, préc., note 43, p. 455. L'auteur fait référence à la Délibération de la CNIL du 7 juin 1983 relative au Fichier central des automobiles.
[389] *Id.*, p. 456.
[390] *Internet, la révolution numérique crée-t-elle une révolution juridique ?*, 1re Rencontres parlementaires sur la Société de l'information et l'Internet, à l'initiative de Christian PAUL, Paris, Éd. M & M Conseil , 1999.

experts, seul le contrôle *a posteriori* des différents programmes effectivement réalisés va permettre à la CNIL de s'assurer de la véritable adéquation entre les finalités générales déclarées et les finalités des applications qui ont réellement été mises en œuvre . Ainsi, par le passé, on pensait déjà au déplacement du contrôle *a priori* vers une forme de contrôle *a posteriori.*

Ce principe, que certains ont qualifié de « moteur de la loi Informatique et Libertés »[391], va servir à « limiter les possibilités de collecte anarchique des données nominatives »[392] et devient un « garde-fou essentiel et souple contre toute collecte inutile et dangereuse »[393].

Afin que ce principe puisse continuer à constituer une limite et un garde-fou, dans les cas où la CNIL identifie l'existence de fortes différences entre les finalités déclarées, la CNIL va plutôt demander la mise en œuvre de traitements distincts.
Dans ce sens, la CNIL s'est félicitée en 2010 de voir que ses recommandations ont été écoutées dans le contexte des fichiers des ex-renseignements généraux[394] et le Gouvernement français a décidé de « créer deux fichiers distincts là où le projet initial consistait en la mise en œuvre d'un fichier unique comportant plusieurs finalités »[395].

Il est essentiel de comprendre sur quels critères se base la CNIL à l'heure d'examiner la conformité d'un traitement pour ce qui est du respect de la finalité. En examinant la doctrine de la CNIL nous constatons qu'elle se fonde essentiellement sur la finalité qui lui a été déclarée par le maître du traitement et pas

---

[391] Nathalie MALLET-POUJOL, *Commercialisation des banques de données*, Paris, CNRS Éditions, 1993, 40.
[392] *Id.*
[393] *Id.*
[394] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *30e Rapport d'activité de la Commission Nationale de l'Informatique et des Libertés*, Paris, La Documentation Française, 2009, p. 22.
[395] *Id.*
L'exemple que la CNIL présente à cet effet fait référence à la distinction qui va devoir être faite dans le secteur bancaire, entre un système de gestion commerciale et un système de lutte contre la fraude.

tellement sur les objectifs qui sont à l'origine de la collecte des données qui ne font pas en l'état actuel l'objet d'une déclaration qui serait différente de celle de la finalité du traitement qui est déclarée[396].

Pour ce qui est de la notion de « l'utilisation compatible ou incompatible », malgré l'existence de la règle de ne pas utiliser les informations à des finalités incompatibles avec la finalité pour laquelle elles ont été collectées, il nous semble difficile de comprendre comment le concept de « compatibilité » se manifeste et se dessine dans l'actualité[397].

**2- La finalité et les interconnexions des fichiers du secteur public**

Comme certains experts l'ont souligné par le passé, les avis défavorables de la CNIL pour ce qui est des traitements mis en place par l'administration sont rares[398]. Ainsi, il a été souligné que la CNIL, d'ordinaire, « rend des avis favorables assortis de réserves et de remarques qu'apparemment l'administration accepte de suivre »[399].

Pour ce qui est des rapprochements de données en général, la CNIL a souligné que « la cession de certains fichiers peut être effectuée en référence au cadre fixé par une norme simplifiée à laquelle le déclarant fait référence »[400], ce qui donne une importance majeure à cet instrument que la CNIL a mis en œuvre et qui garde un rapport important avec la notion même de finalité.

---

[396] Nous constatons alors que la déclaration d'une finalité particulière va déterminer tout ce qui concerne les règles encadrant un tel traitement.
[397] C'est à notre avis une des questions les plus importantes touchant à la problématique de l'utilisation secondaire des informations à caractère personnel.
[398] Herbert MAISL, « État de la législation française et tendances de la jurisprudence relatives à la protection des données personnelles », *Revue internationale de droit comparé*, Vol. 39 n. 3, 1987, 559, 563.
[399] *Id.*, 564.
[400] Alain BENSOUSSAN, *Informatique, Télécoms, Internet*, Levallois, Éditions Francis Lefebvre, 2004, p. 514.

Nous considérons important de souligner ce que la CNIL établit à l'heure de parler de certains rapprochements d'informations et du rôle que joue le principe de finalité au moment d'examiner chaque cas.

Voici comment, en 1982, la CNIL évoque le partage d'informations entre administrations :

> « Les administrations, c'est un fait acquis dans toutes nos sociétés industrialisées, sont demanderesses d'un nombre croissant d'informations, soit qu'elles en ont besoin pour déterminer les conditions d'attribution des prestations qu'elles consentent (Sécurité sociale, Éducation…), soit qu'elles sont investies de missions de contrôle (administration fiscale, police…), soit encore qu'elles éprouvent la nécessité d'établir des prévisions et de dresser le bilan, notamment statistique, de leur action. »[401]

Dans les cas de transmission des données entre administrations, il faut remarquer que la CNIL a déjà rendu une délibération par le passé, interdisant à EDF-GDF, sur la base du principe de finalité, de donner accès global à son fichier d'abonnés[402]. Dans ce cas, ces établissements publics ont déposé une demande de conseil auprès de la CNIL, qui nous rappelle que les établissements publics de cette nature sont régis par un double principe juridique :

> « - principe de spécialité : l'activité des établissements est limitée au service public qu'ils ont pour mission de gérer, ils ne peuvent pas employer leur patrimoine à d'autres fins ;
> - principe de finalité : reconnu par l'article 44 de la loi du 6 janvier 1978, ils ne peuvent utiliser les fichiers qu'ils détiennent (fichiers d'abonnés, de personnel, de fournisseurs) qu'à des fins de gestion personnelle de leurs établissements. »[403]

---

[401] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *3e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1982, p. 190.
[402] *Id.*
[403] *Id.*
Il faut noter que l'article auquel la CNIL fait référence se trouve dans le texte de la Loi Informatique et Libertés avant sa réforme.

La CNIL précise donc qu'il résulte de ces principes que les fichiers d'informations nominatives que les établissements publics de cette nature détiennent, en vue de remplir la mission de service qui leur est impartie, ne peuvent pas être utilisés pour d'autres finalités que celle qui a été déclarée. Pour cette raison, la CNIL a exclu que les fichiers d'EDF-GDF jouent un rôle de « fichier de référence » à disposition de tous ceux qui en feraient la demande.

En tout cas, cette décision de la CNIL établit une doctrine pour ces cas où nous identifions des risques pouvant découler de cession ou d'interconnexion de ces fichiers à une grande échelle. Ainsi, il lui a semblé fondamental ne pas autoriser ces éventuelles interconnexions ou cessions sauf lorsque des dispositions législatives le prévoyaient expressément et, par ailleurs, il a fallu préciser que les demandes du secteur public ne devaient en aucun cas aboutir à la communication ou à la transmission de fichiers complets ou de sous-ensembles de fichiers.

Il s'agissait notamment à cette occasion du fichier des abonnés, mais la doctrine de la CNIL s'applique à l'ensemble des fichiers et, en particulier, aux fichiers de gestion du personnels et des fournisseurs. Pourtant, nous observons que, plus tard, la CNIL a continué à élaborer une doctrine après avoir pu observer un certain laxisme dans l'utilisation des fichiers de gestion, qui sont parfois utilisés à des fins de prospection politique ou électorale.

Quelques années plus tard, le problème est réapparu dans le cadre d'un dossier relatif au détournement de finalité du fichier du personnel d'EDF-GDF, qui avait fait l'objet d'une communication par extraits à divers destinataires. La CNIL a adressé à cette occasion[404] un avertissement public aux organismes responsables et destinataires de ce fichier EDF-GDF visant à adopter des mesures de sécurité et des précautions afin de préserver les informations nominatives qu'ils détiennent.

---

[404] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n° 84-40 du 20 novembre 1984 relative au détournement du fichier de gestion du personnel sur ordinateur d'EDF-GDF*.

La CNIL a voulu également rappeler l'interdiction qui est faite d'utiliser des fichiers à des fins qui ne correspondent pas à celles qui ont été déclarées.

Une des questions les plus importantes entourant la communication des renseignements personnels est celle relative aux données collectées par le service public. En effet, la CNIL établit une doctrine relative à l'utilisation des traitements mis en œuvre par les personnes en charge d'une mission de service public à des fins étrangères à cette mission. Elle rappelle également que ces fichiers, comme celui des abonnés EDF-GDF, peuvent susciter la convoitise, puisqu'ils ont un caractère exhaustif, qu'ils sont tenus à jour et qu'ils ne contiennent que des informations fiables et exactes[405].

Il faut noter également que des « tiers autorisés » peuvent avoir accès à ce type de fichiers et il revient dans ce cas au responsable du fichier de réserver une suite favorable à leurs demandes. Comme la doctrine nous le rappelle, ce tiers autorisé constitue une notion « au maniement délicat »[406]. Dans tous les cas, si l'acte de création du traitement mentionne la liste des destinataires, certaines administrations disposent d'un pouvoir d'investigation qui leur permet d'accéder à des fichiers.

Certaines conditions s'appliquent toutefois à ce type de demandes d'accès : elles doivent être ponctuelles, elles ne doivent porter que sur des informations individualisées et elles ne doivent pas aboutir par leur fréquence et leur importance à « la communication ou à la transmission de fichiers ou des sous-ensembles de fichiers, pas plus qu'à la mise en place d'interconnexions »[407].

Il convient à cet égard, de regarder la situation de l'administration fiscale, puisque même si elle est un « tiers autorisé », certains se demandent si elle peut à ce titre requérir des copies entières de fichiers, question qui ne se pose plus puisqu'elle ne

[405] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 171, p. 59.
[406] H. MAISL, préc., note 398, 572.
[407] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 171, p. 60.

peut que procéder à des relevés ponctuels pour des personnes identifiées, soit à des relevés portant sur les personnes pouvant être en relation avec les contribuables concernés[408].

Mais, plusieurs questions restent sans réponse, comme celle visant à savoir dans quelle mesure un organisme soumis au droit de communication peut être obligé à opérer des traitements de tri ou de sélection : « Les facilités nouvelles qu'offre l'informatique à l'administration ne doivent pas rompre l'équilibre difficile à réaliser entre les prérogatives de celle-ci et les garanties du contribuable »[409].

Toutefois, il faut noter que la CNIL considère comme légitime l'utilisation de l'informatique pour rendre la gestion administrative plus efficace dans les cas où les citoyens bénéficient de garanties. La CNIL ne voit aucune objection quand il s'agit d'améliorer la gestion administrative par le biais de certains systèmes informatisés à condition qu'aucune décision administrative ne soit prise sur la base du seul traitement automatisé et que les intéressés puissent connaître et contester les informations et raisonnements utilisés dans les traitements automatisés dont les résultats leurs sont opposés[410].

La CNIL signale que sa doctrine est parfois mal comprise et elle est accusée de se complaire dans une interprétation purement abstraite de la Loi I et L. Toutefois, il s'agit pour elle de signifier que « le principe de finalité d'un fichier est un principe essentiel au respect de libertés publiques et qui doit s'imposer avec d'autant plus de force que le fichier revêt un caractère public »[411].

En tout cas, pour ce qui est du fichier EDF-GDF notamment et pour les fichiers à caractère public en général, la CNIL nous rappelle la raison de sa position de principe défavorable à la communication à des tiers des données qu'ils contiennent.

---

[408] H. MAISL, préc., note 398, 573.
[409] *Id.*
[410] *Id.*, 569.
[411] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 171 p. 60.

Et cela parce que normalement ces fichiers revêtement deux caractéristiques d'importance : ils constituent des fichiers de service public et, à ce titre, ne doivent pas être utilisés à des fins étrangères au « service public »[412], et d'autre part, il s'agit de fichiers à « clientèle captive »[413], dans la mesure où il n'est pas possible d'obtenir certains services sans figurer dans ce fichier.
Ces raisons expliquent les mesures de protection *ad hoc* pour les fichiers de service public et les précautions prises lors de possibles utilisations à des fins étrangères au service public.

Nous constatons que c'est dans les cas de rapprochement d'informations que le principe de finalité devient un principe fondamental à l'heure d'évaluer les dossiers. Regardons par exemple comment la CNIL s'exprime à cet égard quand il s'agit d'analyser les conséquences d'une éventuelle utilisation du fichier de la taxe d'habitation par l'INSEE pour le recensement de la population de 1982. Dès mars 1981, il avait été question de créer des traitements automatisés d'informations nominatives effectués sur la base d'informations collectées à l'occasion du Recensement général de la population de 1982[414]. À cette occasion, la CNIL a considéré que le rapprochement de ce fichier avec celui des taxes d'habitation ne pouvait avoir lieu sans que soit effectuée une nouvelle demande.
Par rapport à l'application du principe de finalité dans ce contexte, la CNIL souligne :

> « Or, malgré les précautions prises, ce rapprochement impliquait l'utilisation d'un fichier fiscal dont la finalité n'était pas prévue à cet effet. Le principe de finalité étant considéré par le législateur comme un principe fondamental dont dépendent les garanties

[412] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 171 p. 61.
[413] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *15e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1994, p. 33.
[414] COMMISSION NATIONAE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n° 81-03 du 10 mars 1981, portant avis relatif à la création de traitements automatisés d'informations nominatives effectués sur la base des informations collectées à l'occasion du recensement général de la population de 1982.*

> complémentaires prévues par la loi, une demande d'avis particulière était nécessaire. »[415]

Plus tard, en décembre de 1981, la CNIL considérant que l'utilisation ainsi prévue n'était pas conforme à la finalité prévue pour l'exploitation du fichier de la taxe d'habitation, a rendu un avis défavorable quant à la mise en œuvre du traitement[416].

La CNIL est particulièrement vigilante sur le respect de ce principe, puisque son détournement constitue selon elle un risque majeur pour les libertés.
Elle nous rappelle que la tentation de créer un fichier de population a toujours été présente par le passé et que « le respect du principe de finalité est par ailleurs de nature à éviter ces errements passés particulièrement dangereux pour les libertés individuelles, un traitement devant être toujours créé pour une finalité particulière qu'il doit servir »[417].

En 1989, le 10e Rapport de la CNIL signale que, à côté de la création des grands répertoires de population, existe également la tentation d'interconnecter au niveau local les différents fichiers :

> « Les mairies, du fait des pouvoirs qui leur sont reconnus, sont un lieu possible de concentration des informations sur l'individu. Il ne faudrait pas que de petits SAFARI locaux se substitue à un grand SAFARI national désormais écarté. »[418]

Même si la crainte de la création d'un nouveau SAFARI existe depuis toujours, il faut remarquer que les détournements de finalité ont fait l'objet d'un très grand

---

[415] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 401, p. 23.
[416] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n° 81-118 du 01 décembre 1981, portant avis relatif à l'utilisation du fichier de la taxe d'habitation par l'I.N.S.E.E. pour le recensement de la population en 1982*.
[417] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *10e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1989, p. 19.
[418] *Id.*, p. 20.

nombre de plaintes auprès de la CNIL, les détournements à des fins commerciales étant les plus nombreux, par rapport à ceux à des fins politiques.
Certains fichiers du secteur public ont également été détournés de leur finalité initiale pour faire l'objet d'une utilisation commerciale. Dans les cas où une extension de la finalité est admise par la CNIL, les personnes concernées doivent être informées d'une telle modification, afin de pouvoir si elles le souhaitent, exercer leur droit d'opposition[419].

En effet, la CNIL a examiné l'utilisation de donnés collectées dans le cadre d'une mission de service public à des fins publicitaires ou de marketing direct. Dans ce cas, il faut tenir compte du fait que l'affiliation à une assurance complémentaire étant obligatoire, « la mise en œuvre d'un tel système aurait contraint l'ensemble des personnes concernées à recevoir des renseignements publicitaires alors que ni la finalité du fichier, ni la mission de service public dont sont investies les caisses ne le justifiaient »[420].

En effet, normalement, les données contenues dans les fichiers publics sont nécessaires à l'obtention de certains services ou de prestations de la part de l'administration, ce qui oblige d'une certaine manière les citoyens à leur fournir un grand nombre de renseignements. Nous pouvons comprendre dans ce contexte pourquoi la CNIL établit le double critère de la finalité du fichier et de la mission de service public pour justifier son avis défavorable dans les dossiers de cette nature.
Il faut noter qu'auparavant la CNIL appréciait au cas par cas ce type de demandes et qu'elle ne les autorisait qu'à titre exceptionnel, sous des conditions très strictes. Suite à la réception de plusieurs demandes de cette nature faisant appel à la générosité publique, la CNIL a décidé de faire prévaloir le respect du principe de finalité des traitements en affirmant très clairement que les fichiers des

[419] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *11e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1990, p. 33 et s.
[420] *Id.* (nous soulignons).

administrations publiques ne pouvaient servir à d'autres fins que celles qui ont motivé leur création.

Dès 1995, la CNIL a fait remarquer que les principales difficultés que soulève le développement des échanges d'informations sur des réseaux internationaux de communication, comme Internet, sont intimement liées à « l'absence de confidentialité et à la liberté totale de circulation et d'utilisation de l'information »[421]. À cette occasion la CNIL affirme qu'il est devenu très difficile de contrôler le respect de certains principes, notamment celui de la finalité, puisque les possibilités d'utilisation dérivée des informations sont multiples.

La CNIL accorde depuis toujours une attention particulière aux interconnexions et, très concrètement, à celles qui se réalisent entre fichiers à finalités distinctes. Il faut souligner que dans le passé, confrontées au besoin de lutter contre la fraude, et plus particulièrement la « fraude fiscale » et la « fraude aux prestations sociales »[422], la plupart des administrations des pays développés ont instauré des dispositifs visant à rapprocher des données contenues dans les fichiers qu'elles détiennent. Ainsi, certaines études nous prouvent que, même si un principe général d'interdiction du transfert de données nominatives entre administrations existe dans la plupart des législations étrangères, cela n'empêche pas l'organisation d'opérations de rapprochement des données fiscales et sociales[423].

En 1998, trois ans après l'adoption de la Directive 95/46/CE, la CNIL a fait des propositions qui ont renforcé, rejoint ou complété celles qui avaient été faites par la Mission Braibant quant à la transposition de ce texte européen.[424] La CNIL veut s'assurer des conditions de mise en œuvre des traitements susceptibles de présenter

---

[421] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *16e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1995, p. 82.
[422] Voir à ce sujet : SERVICE AUX AFFAIRES EUROPÉENNES, SÉNAT FRANÇAIS, *L'interconnexion des fichiers administratifs*, Juin 1999, p. 1.
[423] *Id.*
[424] G. BRAIBANT, préc., note 56.

des risques particuliers au regard des droits et libertés des personnes concernées, qu'ils soient d'origine publique ou privée.

Plus particulièrement, elle faisait référence à l'article 20 de la Directive 95/46/CE qui prévoit que les traitements de cette nature doivent faire l'objet d'un examen préalable. La CNIL offre une liste des traitements qui, à son avis, doivent appartenir aux catégories soumises aux formalités de l'article 20 de la Directive 95/46/CE et, en conséquence, ne peuvent pas faire l'objet d'une exonération de notification ou d'une simplification des procédures déclaratives, comme une simple déclaration du traitement. La liste contient un ensemble de catégories parmi lesquelles on retrouve l'« interconnexion entre fichiers à finalité distincte », comme étant une de celles qui présentent des risques particuliers devant être encadrés de façon à ne pas limiter les droits et libertés des personnes concernées. La Loi I et L modifiée est venue donner réponse à cette volonté de la CNIL, comme nous avons pu le constater dans les pages précédentes.

### 3- Numéro d'identification national et échanges de données personnelles entre administrations

Toutefois, les questions entourant les interconnexions des fichiers de différentes natures et à finalités distinctes se compliquent davantage quand les échanges se produisent grâce à l'utilisation du numéro national d'identification, NIR.
Même si plusieurs croisements de fichiers au sein de l'Administration sur la base du NIR avaient déjà été autorisés dans le passé, le projet d'extension du NIR à la sphère fiscale a soulevé de grandes inquiétudes au sein de la CNIL en 1997.
En effet, la CNIL a été une nouvelle fois saisie pour le cas d'une disposition devant figurer dans un projet de loi portant diverses dispositions d'ordre économique et financier et qui posait le principe des échanges automatisés d'informations entre les organismes de la sécurité sociale et l'administration fiscale et autorisait celle-ci à

disposer du NIR[425]. Même si finalement ce projet n'a pas été adopté et la délibération de la CNIL à ce sujet n'a pas reçu d'application, les réserves que la CNIL avait émises fournissent une importante doctrine en cette matière.

Ainsi, la CNIL nous rappelle que l'une des motivations de l'adoption de la Loi I et L a été d'éviter qu'une personne puisse être identifiée par un même numéro commun à diverses administrations, de même que le fait que les identifiants nationaux comme les interconnexions de fichiers publics doivent faire l'objet d'une protection particulière, notamment quand il s'agit d'interconnecter des fichiers publics[426].

La CNIL a exprimé à cette occasion sa crainte quant à la généralisation d'un identifiant commun à des organismes de nature très différente, pouvant faire courir le risque qu'à des périodes où les principes démocratiques ne seraient plus respectés ou garantis, un même critère d'interrogation des fichiers administratifs pourrait, sur cette seule information, les révéler toutes, faisant du NIR un identifiant national unique[427].

C'est en 1998 que la CNIL consacre une grande partie de son Rapport annuel à exposer sa doctrine sur le principe de finalité grâce à l'étude des questions permettant de parcourir sa position au fil des années. Ces questions représentent la problématique entourant l'application de ce principe et montrent les enjeux majeurs auxquels la CNIL a dû faire face dans le passé.

Nous avons pu observer que le développement de l'administration électronique suppose l'introduction d'un nouveau dossier dans lequel le principe de finalité se trouve face à des difficultés tirant leur origine d'un nouveau modèle de circulation des renseignements personnels.

---

[425] Cette disposition allait permettre de vérifier systématiquement auprès de l'administration fiscale les ressources déclarées par les personnes s'adressant aux organismes sociaux pour solliciter des allocations subordonnées à condition de ressources.

[426] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n° 97-021 du 25 mars 1997 portant avis sur un projet d'article L. 115-8 du code de la sécurité sociale.*

[427] *Id.*

La CNIL fait notamment référence aux interconnexions et au NIR, deux questions qui se trouvent au centre des réflexions de la CNIL depuis la mise en place d'un système de protection des renseignements personnels en France. Fin 1998, un amendement à la loi des finances en France avait été adopté, ce qui autorisait les administrations financières à collecter, conserver et transmettre le NIR. Vingt ans après SAFARI, la CNIL revient sur les éléments de doctrine définis dans ce domaine pour souligner quelques idées qui ont aujourd'hui encore toute leur actualité.

Il est rappelé surtout que la Loi I et L est rigoureuse pour ce qui est des fichiers de nature publique qui ne peuvent être mis en œuvre qu'après avis favorable de la CNIL ou après intervention d'un décret en Conseil d'État pour passer outre à un avis défavorable, tandis que les fichiers privés ne font l'objet que d'une simple procédure de déclaration, ce qui prouve les inquiétudes provoquées par la puissance des pouvoirs publics.
C'est une idée de grande importance qui est soulignée quand la CNIL affirme que les interconnexions de fichiers « sont assimilées à des véritables traitements qui doivent, en tant que tels, être subordonnées à l'avis de la CNIL »[428].

Mais il est rappelé également que pour l'utilisation du Répertoire national d'identification des personnes physiques (RNIPP), associant à chaque personne un numéro d'identification spécifique et signifiant, un décret en Conseil d'État après avis de la CNIL est nécessaire.

En général, dans le domaine fiscal et social, les rapprochements de fichiers résultent de dispositions législatives spécifiques, devant préciser les finalités de ces rapprochements. La CNIL, dès que certaines conditions sont respectées, va habituellement admettre que les fichiers sont interconnectés si un intérêt public le justifie.

---

[428] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *19e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1999, p. 40.

Ainsi, comme condition essentielle, la CNIL vérifie si les informations sont protégées par le secret professionnel ou par un secret particulier, tel que le secret médical ou fiscal. Dans ces cas, le partage de ces informations ou leur divulgation à un organisme tiers ne peut se réaliser que si ce secret a été préalablement levé par la loi. La CNIL énonce un principe fondamental en affirmant que l'informatique ne doit pas permettre de faire ce que le législateur a entendu proscrire. L'échange d'informations couvertes par un secret ne peut intervenir que si ce secret a été préalablement levé.

Regardons par exemple la mise en œuvre d'interconnexions ayant pour but de vérifier la réalité de la situation administrative ou socio-économique de certains bénéficiaires de prestations. Pour ce qui est des interconnexions entre les différentes administrations une deuxième condition s'impose, ayant comme principe essentiel de servir à ce que les personnes concernées soient convenablement informées.
La CNIL ne conteste pas la légitimité de cet objectif de contrôle, mais des précautions particulières s'imposent : l'État a une obligation de loyauté à l'égard des citoyens, qui ne peuvent pas être tenus dans l'ignorance de l'interconnexion, constituant également la plus efficace des mesures de prévention aux tentations de fraude. Ainsi, la CNIL recommande que la mise en place de ce type d'interconnexion s'accompagne d'une exacte information des personnes concernées à cet effet.

Finalement, la CNIL vérifie si ces opérations de rapprochement se traduisent par une réelle simplification des démarches administratives et elle est particulièrement vigilante également sur les mesures de sécurité devant entourer ces échanges, tels que les contrôles des accès ou le chiffrement des données. En application de l'article 34 de la Loi I et L modifiée, le responsable du traitement est tenu de prendre toutes les précautions utiles pour préserver la sécurité des informations et notamment d'empêcher leur divulgation, créant une obligation de sécurité devant être respectée dans ce contexte particulièrement délicat.

Quant au NIR, la CNIL a toujours manifesté des réticences à ce que, au seul motif d'autoriser les interconnexions, un service de l'administration puisse utiliser le NIR si elle n'a pas été préalablement autorisée à l'utiliser afin de gérer ses propres fichiers, et à ce que le NIR devienne un élément identifiant dans l'ensemble des fichiers de l'administration concernée[429].

Une idée d'ordre technique d'une grande importance est soulignée par la CNIL quand elle affirme que, contrairement à ce qui est très souvent mis en avant à ce sujet, le NIR ne constitue pas la « solution miracle » aux interconnexions, puisque les échanges d'informations, même sur la base du NIR entre deux administrations qui en disposent, connaissent un taux d'échec non négligeable.
La CNIL ajoute une réflexion à cet égard :

> « (…) ces débats manifestent que les interconnexions doivent être étroitement encadrées si l'on souhaite que soit respecté le point d'équilibre défini par toutes les législations de protection des données : le principe de finalité. Les interconnexions ne sont pas interdites par nos législations mais elles constituent incontestablement des exceptions. Et l'exception doit s'interpréter strictement. »[430]

L'idée qui est exprimée ici vise à affirmer que les interconnexions entre les fichiers administratifs ont constitué des exceptions à un régime général, et cela depuis plus de trente ans. C'est pour cela qu'il est essentiel de comprendre comment, dans le contexte de l'administration électronique où les échanges entre les différents services administratifs ont tendance à devenir une pratique habituelle, ces interconnexions seront encadrées. Nous y reviendrons dans les pages qui suivent.

Certainement, la doctrine de la CNIL a contribué au cantonnement du NIR « dans ce qu'il est convenu d'appeler par commodité la sphère sociale »[431], jusqu'au moment où il a été étendu par la loi au domaine fiscal. Au lieu de renoncer à sa

[429] *Id.*, p. 42.
[430] *Id*., p. 46 et 47 (nous soulignons).
[431] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *20e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 2000, p. 62.

doctrine, la CNIL a limité l'utilisation du NIR par les administrations financières à une fonction précise de sécurisation de l'identifiant fiscal, afin que le NIR ne devienne pas un identifiant généraliste, permettant ainsi de nouvelles interconnexions[432].

En plus, dans un souci de meilleure garantie et de précaution, La CNIL « a prolongé le principe de finalité d'un traitement pris dans son ensemble à celui de l'usage spécifique qui pouvait être fait d'une information particulière : le NIR »,[433] afin de refuser toute utilisation non finalisée de ce numéro.
Pour la CNIL, au regard du principe de finalité, le problème le plus important reste celui des interconnexions, suivant le principe essentiel que l'interconnexion ne doit pas être un vecteur de transmission du NIR à une administration qui n'aurait pas été préalablement autorisée à l'utiliser.

Dans le passé, lorsque l'utilisation du NIR a été précédemment autorisée dans les fichiers concernés par une interconnexion, la CNIL a admis que ce numéro puisse être également utilisé afin de réaliser les rapprochements d'informations.
Notons encore que la CNIL s'est prononcée dans le passé favorablement à la mise en place de traitements informatiques liés à l'attribution et à la gestion du Revenu minimum d'insertion (RMI). C'est surtout la crainte de la fraude qui a conduit les pouvoirs publics à compléter ce dispositif d'un fichier national de bénéficiaires du RMI en usant des interconnexions, afin de vérifier la réalité de la situation sociale des demandeurs. Ainsi, des échanges automatisés ont été mis en place entre les Caisses d'allocations familiales, d'autres organismes versant des revenus de remplacement (ASSEDIC, Caisses d'assurance maladie, CNASEA) et les services fiscaux, afin de contrôler l'attribution du RMI[434].

---

[432] *Id.*, p. 63.
[433] *Id.*, p. 65.
[434] Voir : COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 171, p. 169.

La CNIL saisie en 1992 d'un projet de loi portant pérennisation du dispositif RMI, avait donné un avis favorable pour permettre des interconnexions au niveau national et de façon permanente.
Toutefois, elle avait demandé que seuls les organismes participant directement au dispositif puissent devenir les destinataires de ces données, en exprimant ainsi sa préoccupation face à la multiplication « des circuits de diffusion » des informations relatives aux bénéficiaires du RMI.
C'est ainsi que la CNIL a exprimé sa volonté d'éviter que les maires puissent connaître l'identité des bénéficiaires du RMI de leur commune, et cela afin d'éviter que ces informations ne soient détournées de leur finalité initiale à des fins politiques[435].

La CNIL a voulu souligner que la réalisation d'interconnexions n'est cependant pas interdite par principe et que, parfois, « cette sage prudence » qui limite certains rapprochements, est quelquefois « mal comprise de quelques administrations qui en déduisent que la CNIL est par principe hostile aux interconnexions entre fichiers »[436].

La CNIL a autorisé dans le passé un grand nombre de transferts, échanges ou communications entre administrations. À titre d'exemple, nous pouvons ajouter que, en 2004, le nombre de délibérations de la CNIL autorisant l'UNEDIC[437] à échanger ou communiquer certaines données de ses fichiers se sont élevées à 28. Bien sûr, les finalités de ces opérations, autorisées par la CNIL, sont de natures très diverses et comportent à plusieurs reprises l'utilisation du NIR ainsi que la vérification de certaines informations concernant les assurés.

D'une part, la nature et le sens des échanges sont très variés et peuvent concerner tant la collecte et le transfert d'informations, que l'accès à certaines informations, des échanges réciproques de renseignements, des rapprochements d'informations,

[435] *Id.*, p. 170.
[436] *Id.*, p. 172.
[437] L'UNEDIC est chargé d'assurer la gestion de l'Assurance chômage.

des transmissions automatisées, la création d'un fichier commun, la consultation de fichiers ou l'assurance des échanges d'informations.

D'autre part, le fondement juridique à la base de ces délibérations est de nature très variée et les délibérations répondent parfois à des demandes d'avis présentées auprès de la CNIL et, exceptionnellement, font suite à des plaintes.

Pour ce qui est des destinataires des données personnelles dans le secteur public en France, H. Maisl affirme en 1987 que, de façon générale, il n'y a pas de secret partagé entre administrations. Il soutient l'idée que : « De surcroît, la législation informatique et libertés vise à renforcer les cloisonnements à l'intérieur d'une même personne morale et à ne laisser communiquer l'information qu'aux agents dont la mission correspond à la finalité du traitement »[438], sans oublier de nous rappeler que « la tendance au décloisonnement et à la banalisation des données »[439] reste vive.

Regardons maintenant comment la CNIL détermine qui sont les destinataires des données personnelles à l'intérieur du service gestionnaire et de service à service.
Si nous regardons comment se partagent les informations entre les membres d'un même service gestionnaire, nous observons que l'accès aux données est réservé aux agents qui en ont besoin, relativement à leurs fonctions ou aux besoins du service[440].
Pour ce qui est de l'accès aux données de service à service, les transmissions sont soigneusement vérifiées et uniquement autorisées pour les fonctionnaires des autres

[438] H. MAISL, préc., note 398, 572 (nous soulignons).
[439] *Id.*
[440] *Id*.
Cet auteur nous rappelle que cette conception a conduit la CNIL dans le passé à se montrer défavorable à la création dans les grandes villes de fichiers permanents nominatifs de la population regroupant l'ensemble des informations nominatives que les différents services détiennent sur les citoyens, afin d'éviter qu'elles soient accessibles à tous les agents de la mairie. Cette même logique a été appliquée dans les cas relatifs à la consultation de données médicales et dans le cadre des projets de médicalisation du système d'informatisation en milieu hospitalier.

services dans les cas où ils ont été dûment habilités, en vertu d'une habilitation strictement personnelle, à un caractère temporaire et révocable.
Dans d'autres occasions, le destinataire n'a accès qu'aux seules catégories d'information nécessaires à l'exercice de ses attributions. Il reste à voir si ces précautions, qui ont été adoptées pour l'accès à des fichiers spécialement sensibles[441] tels que ceux liés à des questions de sécurité nationale, s'appliquent dans tous les cas ou si les conditions d'accès sont moins exigeantes pour les fichiers contenant des informations moins sensibles.

Cette question est très fortement liée à celle de l'utilisation des identifiants permettant de relier de très grands fichiers publics, qui résultent eux-mêmes de dispositions législatives ou réglementaires de portée nationale. La CNIL a toujours exprimé le besoin d'utiliser des identifiants spécifiques à chaque secteur, identifiants associés à leur objet et réservés à cet usage exclusif.
Cependant, pour la CNIL, les interconnexions internes au secteur ne sont pas autorisées *ipso facto* et la CNIL va devoir décider dans chacun des cas. Il est en effet important de souligner que, dans chaque secteur, les interconnexions ne peuvent se réaliser que sous la surveillance de la CNIL, qui va devoir décider selon les cas[442].

**4- L'extension de finalité et le détournement de finalité**

C'est dans son 2e Rapport annuel que la CNIL souligne que dans certaines délibérations on voit apparaitre la notion « d'extension de finalité »[443], ainsi que celle de « détournement de la finalité »[444].

---

[441] Tel est le cas du fichier « violence-attentat-terrorisme », détenu par les services des renseignements généraux, accessible aux fonctionnaires d'autres services de défense et de la police. Voir : H. MAISL, préc., note 398, 572.
[442] Ce principe peut en effet limiter les interconnexions de fichiers à l'intérieur d'un même service ou section d'un organisme public, interconnexions qui doivent toujours être guidées par la finalité de chaque traitement et non par des critères à caractère « organisationnels ».
[443] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération nº 81-03 du 10 mars 1981 portant avis relatif à la création de traitements automatisés*

La CNIL a créé une sous-commission « Recherche »[445] en 1981, qui a réalisé des travaux sur la question de l'équilibre entre les intérêts de la recherche et le droit à la protection des données personnelles. Des demandes d'avis traitées et des travaux suivis par cette sous-commission mettent en exergue des éléments de doctrine concernant le principe de finalité fort intéressants.

Cette sous-commission analyse les cas de détournement de finalité pour lesquels les données ont été recueillies, traitées et conservées. Pour favoriser la conciliation des intérêts en présence, « la sous-commission a été amenée à dégager le principe de l'extension de finalité »[446]. La CNIL émet des « réserves à l'égard des finalités évolutives »[447] et elle réclame des précisions dans la formulation des finalités afin d'éviter les finalités évolutives pouvant porter préjudice aux personnes concernées[448].

La CNIL élabore dès 1981 la théorie de l'extension de la finalité, toutefois « le principe de finalité, tel qu'il est appliqué par la CNIL, est ressenti par de nombreux chercheurs comme une entrave au développement de leur activité »[449].

---

*d'informations nominatives effectués sur la base des informations collectées à l'occasion du recensement général de la population de 1982.*
La CNIL dans cette délibération considère que dans le cas de ce fichier, il se produit une extension de finalité qui ne peut pas être admise par la CNIL sans qu'une demande d'avis spécifique lui soit soumise.

[444] *Id.* Ainsi encore dans cette Délibération, la CNIL demande que des « précautions techniques soient envisagées contre tout risque de détournement de finalité ».
Il est important de souligner que la CNIL établit également dans son 2e Rapport, une doctrine quant à cette notion de « détournement de la finalité » en soulignant que si un détournement de finalité portant sur des informations collectées dans un autre but est porté à la connaissance de la Commission, elle s'informe de la réalité des faits. Ce n'est que dans la mesure où le détournement serait caractérisé qu'elle en ferait part au parquet. Son intervention n'est en aucun cas obligatoire, et le plaignant peut saisir directement le ministère public ».

[445] Cette sous-commission a été créée lors de la réunion de la CNIL le 17 novembre 1981 et était animée par Mme Cadoux, conseiller d'État.

[446] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *3e Rapport d'activité de la Commission Nationale de l'informatique et des libertés, Paris, La Documentation Française*, 1982, p. 148.

[447] I. DE LAMBERTERIE et H.-J. LUCAS (dir.), préc., note 31, p. 80.

[448] Voir à ce sujet : COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 379, p. 37.

[449] I. DE LAMBERTERIE et H.-J. LUCAS (dir.), préc., note 31, p. 80.

En ce qui concerne l'application du principe d'extension de finalité, la sous-commission établit des critères très différents, et cela en fonction du type de données. Dans certains cas, comme dans celui de la constitution des échantillons dans le cadre d'une recherche à partir de fichiers administratifs lorsque l'objet du traitement envisagé se situe « dans le champ d'application ou le prolongement de la finalité du fichier de base », les garanties exigées consistent à demander aux chercheurs qu'ils informent les personnes soumises à l'enquête du mode d'obtention de leur adresse, ainsi qu'à limiter la durée de conservation des données nominatives.

Notons que cette expression concernant le prolongement de la finalité quant au fichier de base, détermine la position que la CNIL adopte par rapport aux conditions dans lesquelles peut se produire une telle extension de la finalité. Nous observons que, dans d'autres cas, la CNIL a considéré que cette extension de finalité ne pouvait pas être accordée ou que le consentement des personnes concernées était nécessaire[450].

Dès 1982, la CNIL établit également que certaines transmissions de données, dans le cadre d'une recherche et en application de la notion de l'extension de finalité, quand le consentement des personnes ne peut pas s'exercer, doivent se réaliser avec des données qui ne sont pas directement nominatives[451].

Il est important de noter que ce principe d'extension de finalité, dégagé du contexte de la recherche, va être appliqué en fonction, d'une part, de la nature des fichiers contenant les renseignements personnels et, d'autre part, du champ de la finalité ou du prolongement de la finalité du traitement.

---

[450] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 401, p. 148.
Ainsi, afin d'éviter que certaines utilisations du fichier électorale puissent lui conférer le caractère d'un registre de population, la CNIL a refusé l'accès à des données dans le cadre d'une recherche. Dans les cas où les fichiers sont couverts par le secret professionnel, la CNIL a considéré que le consentement des personnes concernées était nécessaire afin de délier l'organisme en question.

[451] *Id.*, p. 150.

Dans nos travaux, nous aurons l'occasion de nous intéresser plus particulièrement, aux difficultés que présente l'examen de ces questions entourant l'utilisation ultérieure des données personnelles.

Cependant, il faut noter que la CNIL, avant d'autoriser des extensions de finalité, veille à ce que des garanties sérieuses soient apportées en ce qui concerne notamment « le respect du secret professionnel, l'anonymisation des données et l'information préalable des personnes »[452]. Un traitement a en principe une finalité unique, ce qui fait que la CNIL est très stricte sur les possibilités d'extension des finalités si l'objet du traitement envisagé se situe dans « le prolongement de la finalité du fichier de base »[453]. C'est ici que l'on éprouve sans doute des difficultés à l'heure de déterminer les cas où effectivement l'on se retrouve face au prolongement du fichier pouvant être à l'origine d'une extension de finalité.

Le contexte de la recherche a permis à la CNIL de dégager une très importante doctrine sur le « principe de séparation fonctionnelle » visant à limiter la réutilisation des informations collectées :

> « (…) Dans telles circonstances, outre l'application des principes de l'extension de finalité et du consentement préalable éclairé des personnes, la question se pose de savoir quel usage ultérieur il peut être fait, par les services administratifs, des données ainsi collectées. En particulier, ces données peuvent-elles être utilisées à des fins de décision et de contrôle individuel ? »[454]

Selon la CNIL, la séparation fonctionnelle des traitements doit être considérée comme un fil conducteur pour la réflexion, « d'une part, elle garantit les intéressés contre le risque que, sous couvert de recherche, d'autres buts ne soient poursuivis,

---

[452] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 379, p. 38. Ainsi, nous pouvons constater comment par exemple, la CNIL a jugé que le fichier électoral ne pouvait pas avoir pour finalité une campagne de dépistage du cancer du sein, alors que les fichiers des caisses d'assurance maladie pouvaient se prêter à une telle utilisation.

[453] H. MAISL, préc., note 398, 570.

[454] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 379, p. 49.

d'autre part, elle apporte aux chercheurs la sincérité et la qualité des données recueillies »[455].

Pour ce qui est du domaine de la recherche, la CNIL, dans les cas de collectes conjointes de données issues de fichiers administratifs et d'entretiens auprès des personnes, établit que le principe est celui de la « séparation fonctionnelle » des traitements, puisque les organismes concernés s'engagent à ne pas utiliser les données recueillies à d'autres fins que celle de l'étude projetée[456].

Ce principe de séparation fonctionnelle est d'une grande actualité dans le cadre de l'utilisation des informations des fichiers administratifs dans le contexte de l'administration et, plus particulièrement, dans celui de l'administration électronique. Ainsi, ce principe appliqué au contexte de la recherche sera essentiel quand nous examinerons par la suite comment les informations sur les citoyens doivent être utilisées afin d'offrir aux citoyens des prestations électroniques de services, grâce à l'utilisation de données personnelles contenues dans des différents traitements au sein de l'administration.

Certains auteurs nous rappellent que la CNIL prend position de manière stricte sur les traitements de données personnelles mis en œuvre par les organismes du secteur public, en considérant que leur finalité doit être « uniquement limitée au service public »[457].

Toutefois, la CNIL n'hésite pas à affirmer que le « détournement de finalité » et « l'extension de finalité » sont deux aspects de la notion de finalité faisant appel à sa vigilance et qui sont à la base de toute sa jurisprudence.

Pour ce qui est du détournement de finalité, la CNIL a pour démarche habituelle de veiller systématiquement à la pertinence des informations au regard de la finalité

[455] *Id.*
[456] C. MARLIAC-NÉGRIER, préc., note 43, p. 461.
[457] A. BENSOUSSAN, préc., note 400, p. 497.

déclarée. La CNIL manifeste toujours « le souci d'une adéquation réelle entre la finalité énoncée et les incidences volontaires ou involontaires que pourrait avoir un tel traitement »[458]. Ainsi, nous devons souligner que l'élément matériel de l'infraction relative au détournement de finalité est constitué par l'utilisation du fichier à une fin autre que celle initialement déclarée à la CNIL [459].

La CNIL va attacher une grande importance à l'examen des catégories d'informations traitées et va retenir uniquement comme indispensables celles qui sont nécessaires à la finalité poursuivie, qui doit demeurer en conformité avec la loi.

Il faut noter que, pour certains auteurs, le détournement de finalité ne consiste pas en une modification quelconque de la finalité « comme l'adjonction d'une finalité supplémentaire et complémentaire mais en un rajout de finalité différente »[460]. Toutefois, pour d'autres, « cette distinction paraît difficile à mettre en œuvre et paraît plutôt être une source de litiges en cas mise en place effective », tout en étant préférable de « respecter la finalité initiale déclarée et de procéder si besoin à une nouvelle déclaration auprès de la CNIL »[461].

Afin de respecter le principe de finalité licite, la CNIL va émettre un avis défavorable quand elle juge que la finalité principale du traitement est contestable. Mais elle va encore plus loin en affirmant que les fichiers doivent correspondre à une finalité licite et être en rapport avec la fonction de l'administration en cause, afin de renforcer ce critère[462].

Bien entendu, la CNIL limite le recueil des renseignements contenus dans les fichiers exclusivement à ceux qui répondent à l'objectif poursuivi par le traitement. Même si l'interdiction d'enregistrer certaines « données sensibles » existe, lorsque

---

[458] *Id.*, p. 218.
[459] Il faut noter que ce détournement de finalité est encadré par le droit pénal et il est passible de peines d'emprisonnement ainsi que d'amendes.
[460] Voir sur les avis de certains auteurs : C. MARLIAC-NÉGRIER, préc., note 43, p. 459.
[461] *Id.*
[462] *Id.*, p. 219.

la collecte de ces informations est pertinente au regard de la finalité, la CNIL autorise un tel enregistrement.

Afin d'encadrer les informations pouvant fournir une définition du profil de la personne concernée, la CNIL veille « à ce que *l'inconscient collectif de l'administration* ne transforme les fichiers en *réservoirs de suspects* faisant de toute personne assujettie à une activité un coupable en puissance et de tout coupable un récidiviste probable »[463].

Pour ce qui est de l'extension de finalité, la CNIL a une position de principe claire en exigeant, depuis toujours, que toute modification ou extension du champ d'application de la finalité d'un traitement déclaré fasse l'objet d'un nouvel examen de sa part. Ainsi, la CNIL va contester certaines extensions quand la finalité n'est plus conforme à celle qui avait fait l'objet d'une déclaration dans le premier projet de traitement.

Comme certains experts l'ont souligné, la mise en œuvre de la législation I et L a généré, en plus de trente ans d'existence, « un nombre extrêmement limité, pour ne pas dire insignifiant, de décisions de justice, aussi bien au pénal qu'au civil »[464].
Il faut noter que l'absence de jurisprudence peut s'expliquer surtout par le manque de sensibilisation chez les individus, qui n'ont pas encore le réflexe de porter les litiges devant les tribunaux, ce qui, à notre avis, s'amplifie considérablement quand nous parlons de litiges face à l'appareil étatique pouvant découler de la gestion des traitements du secteur public.

Cependant, il faut noter encore que cette absence de jurisprudence en la matière s'explique par « l'existence même de la CNIL, dont l'une des missions est de dénouer les situations de crises et ainsi d'éviter le recours aux juridictions »[465].

---

[463] *Id.*, p. 220 et 221.
[464] GUILLAUME DESGENS-PASANAU, « Informatique et Libertés : une équation à plusieurs inconnues », dans Jean-Luc GIROT (dir.), *Le harcèlement numérique*, Paris, Dalloz,2005,75, p. 103.
[465] *Id.*, p. 104.

**SECTION 2 Le contexte fédéral canadien dans le secteur public**

Nous retrouvons dans la LPRP canadienne, applicable au secteur public fédéral, certaines dispositions renfermant l'esprit du principe de finalité et ayant pour objectif de limiter l'utilisation des renseignements personnels.
Ainsi, selon l'alinéa 7 (2)a), à défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci qu'aux fins pour lesquelles ils ont été recueillis ou préparés par l'institution, de même que pour les usages qui sont compatibles avec ces fins.

Le paragraphe 8(1) établit que pour ce qui est de la communication des renseignements personnels relevant des institutions fédérales, le consentement de la personne concernée sera nécessaire.
Toutefois, l'alinéa 8(2)a) va permettre la communication de renseignements personnels aux fins pour lesquelles ils ont été recueillis ou préparés par l'institution ou pour les usages qui sont compatibles avec ces fins.
Nous observons des dispositions similaires pour ce qui est de l'utilisation et de la communication des renseignements personnels dans le secteur privé, faisant appel au critère des « fins compatibles » comme critère.
Nous allons essayer, dans les pages qui suivent, d'analyser l'interprétation qui a été donnée de cette notion relative à la finalité, afin de comprendre comment ce critère a été utilisé dans le contexte canadien.

Nous verrons également que la LPRP reste parfois inefficace à l'heure de protéger les renseignements personnels dans le secteur public. Le CPVPC affirme que, depuis l'entrée en vigueur de la LPRPDE, applicable au secteur privé canadien, « la pression augmente sans cesse pour que le gouvernement garantisse une protection similaire des renseignements personnels autant dans le secteur public que dans le secteur privé »[466].

[466] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 324, p. 8.

**1- De la notion de « l'usage compatible » aux « fins acceptables » et le test de la « personne raisonnable »**

La notion faisant référence aux usages compatibles avec les fins ayant motivé la collecte des renseignements personnels est une des notions les plus problématiques de la LPRP, loi applicable à tout le secteur public canadien.

Les premières recommandations destinées à la réforme de la LPRP remontent au premier examen exigé par cette Loi[467], lequel a été mené en 1987 avec la publication du Rapport *Une question à deux volets : Comment améliorer le droit d'accès à l'information tout en renforçant les mesures de protection des renseignements personnels*[468]. Il faut souligner que le Gouvernement[469] s'était engagé dans sa réponse à ce Rapport, à apporter des changements au plus tard à l'automne 1988 mais, jusqu'à présent, aucun de ces changements n'a été encore apporté.

Dix ans après son premier examen, un autre comité parlementaire a recommandé qu'une révision importante soit effectuée et depuis plusieurs documents et rapports recommandent une urgente réforme de ce texte de loi[470]. Comme le CPVPC le signale en 2006, si déjà en 2000 l'examen de la loi était inévitable, il l'est d'autant plus à ce moment[471].

Aujourd'hui, en 2010, l'urgence s'accroît à cause de certains phénomènes tels que l'avènement d'Internet et le développement des technologies en général. Toutefois, selon certains, « le cybergouvernement[472] pourrait être le catalyseur de la réforme

[467] Voir à ce sujet : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2005-2006 sur la Loi sur la protection des renseignements personnels*, 2006, p. 12.

[468] STANDING COMITTEE ON JUSTICE AND SOLLICITOR GENERAL ON THE REVIEW OF THE ACCESS TO INFORMATION ACT AND THE PRIVACY ACT, *Une question à deux volets : Comment améliorer le droit d'accès à l'information tout en renforçant les mesures de protection des renseignements personnels*, 1987.

[469] Voir sur les questions entourant la volonté de réformer la LPRP : GOUVERNEMENT DU CANADA, *Accès et renseignements personnels : les prochaines étapes*, 1987.

[470]COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2004-2005 sur la Loi sur la protection des renseignements personnels*, 2005, p. 21.

[471] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2005-2006 sur la Loi sur la protection des renseignements personnels*, 2006, p. 13.

[472] Ce terme est utilisé pour désigner l'Administration électronique.

de la LPRP en vue d'en faire un cadre de gestion de la protection de la vie privée beaucoup plus efficace »[473].

Plus concrètement, c'est aux fins d'utilisation des renseignements personnels que le CPVPC fait référence à l'heure de montrer le besoin de réforme de la LPRP dans le cadre d'un cybergouvernement :

> « La Loi doit prévoir des contrôles plus stricts de l'accès au bassin de renseignements. Une loi efficace devrait aussi exiger en premier lieu une meilleure justification lorsqu'il s'agit de recueillir des renseignements, une justification qui doit être clairement énoncée. Cette loi devrait exiger également une conformité beaucoup plus rigoureuse au principe selon lequel des renseignements personnels doivent être utilisés seulement aux fins pour lesquelles ils sont recueillis. »[474]

Nous constatons alors qu'un renforcement de la LPRP est nécessaire pour ce qui est de l'obligation que les renseignements personnels soient utilisés uniquement aux fins pour lesquelles ils ont été recueillis. Cette urgence est devenue encore plus évidente après l'adoption de la LPRPDE pour le secteur privé puisqu'en effet, « on pourrait remédier à plusieurs préoccupations du Commissariat à la protection de la vie privée en adoptant des dispositions similaires à celles de la LPRPDE »[475].

Il faut souligner encore que la règle générale que l'alinéa 7 (2)a) de la LPRP établit est que, à défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution de même que pour les usages qui sont compatibles avec ces fins.

Si nous analysons le premier examen réalisé à la LPRP en 1987, nous observons que, selon ses auteurs, il a été malheureux que la LPRP ne définisse pas d'avantage ces « usages compatibles ».

---

[473] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 324, p. 14.

[474] *Id.* (nous soulignons).

[475] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 470, p. 21.

Et cela, parce que l'alinéa 8(2)a) qui va permettre la communication de renseignements personnels aux fins pour lesquelles ils ont été recueillis ou préparés par l'institution ou pour les usages qui sont compatibles avec ces fins, risque d'être utilisé « pour contourner l'obligation impérative de réglementer étroitement la communication des renseignements personnels »[476].

Les institutions fédérales canadiennes sont tenues de faire un relevé des « usages compatibles » dans le Répertoire de renseignements personnels qui est publié chaque année. Sinon, l'alinéa 9(4) de la LPRP stipule que le responsable de l'institution est tenu d'aviser immédiatement le CPVPC de l'usage qui a été fait des renseignements ou pour lequel ils ont été communiqués, ainsi que de faire insérer une mention de cet usage dans la liste des usages compatibles dans l'édition suivante du Répertoire.

Le comité ayant réalisé le premier examen à la LPRP dit, en 1987, se préoccuper très sérieusement de ce que le mécanisme de contrôle des usages compatibles institué par la LPRP ne semble pas fonctionner de façon efficace[477].

Ce Comité affirme que cette notion présente dans le droit canadien est dérivée de la notion « d'usages courants » qui se trouve dans la législation américaine, notion problématique que, selon des experts américains, il faut interpréter grâce à d'autres critères[478].

Ainsi, dans le contexte américain, il a été affirmé que la « compatibilité » est la seule norme sur laquelle les organismes américains se basent pour décider si la communication peut se faire à des fins courantes.

Il a été recommandé également que, outre ce critère de « compatibilité », les usages courants soient également conformes aux conditions ou « attentes raisonnables » en

---

[476] STANDING COMITTEE ON JUSTICE AND SOLLICITOR GENERAL ON THE REVIEW OF THE ACCESS TO INFORMATION ACT AND THE PRIVACY ACT, préc., note 468, p. 66.

[477] *Id.*, p. 67.

[478] *Id.*

Le Comité fait plus exactement référence à la Loi sur la protection des renseignements personnels des États-Unis.

matière d'utilisation et de communication en vertu desquelles l'information contenue dans le dossier a été fournie[479]. Nous observons alors que le critère de la compatibilité éprouve des difficultés, par lui seul, à fournir des réponses capables de déterminer la légitimité de certains usages des renseignements personnels.

Pour ce qui est du contexte canadien, le Comité a recommandé que l'on intègre une définition de l'expression « usage compatible » à la LPRP, faisant référence au critère selon lequel l'usage ou la communication des renseignements personnels doit avoir un « lien pertinent et direct» avec les fins premières pour lesquelles le renseignement a été recueilli.
Le Comité propose en 1987 la définition suivante :

> « "Usage compatible" s'entend, en ce qui concerne la communication d'un document ou de renseignements personnels, de tout usage qui est conforme aux fins pour lesquelles le document ou les renseignements ont été recueillis, et qui est nécessaire à l'institution qui a recueilli ou obtenu le document ou les renseignements personnels pour s'acquitter des ses responsabilités statutaires ou pour exploiter un programme expressément autorisé par la loi. Un usage ne peut être compatible que s'il a un lien pertinent et direct avec les fins premières pour lesquelles le document ou les renseignements ont été recueillis ou consignés. »[480]

Cette définition n'a jamais été insérée dans la LPRP et la notion d'usage compatible a évolué lors des dernières années. Le SCT a joué un rôle majeur dans l'évolution de cette notion au fil des années. Ainsi, le SCT a eu recours également à une conception des usages compatibles appuyée sur un lien pertinent et direct avec les fins premières pour lesquelles ces renseignements ont été recueillis.
Le SCT a élaboré un guide d'usage et de communication de tous les renseignements personnels relevant des institutions fédérales, où il est encore allé plus loin, afin d'aider à fixer les contours de cette notion, en établissant quel est le moyen le plus adéquat pour savoir si un usage ou une communication prévus sont

[479]Voir sur le contexte américain : STANDING COMITTEE ON JUSTICE AND SOLLICITOR GENERAL ON THE REVIEW OF THE ACCESS TO INFORMATION ACT AND THE PRIVACY ACT, préc., note 468, p. 67.
[480] *Id*., p. 68 (nous soulignons).

compatibles : « (...) consiste pour la personne qui a fourni les renseignements, à se demander s'il est raisonnable de s'attendre à ce que les renseignements fournis soient utilisés de la façon dont on se propose de le faire »[481].

Le SCT ajoute : « En d'autres termes, les fins premières est les fins prévues sont si intiment liées que la personne s'attend à ce que les renseignements soient utilisés à une fin compatible, même si l'usage n'est pas expressément indiqué ».

Dernièrement, le SCT a rendu publique une Politique sur la protection de la vie privée[482], entrée en vigueur en 2008, applicable aux institutions fédérales. Nous retrouvons dans ce texte une définition de l'usage compatible introduisant de nouveaux éléments : « Usage compatible ou *Consistent use* (en anglais) est un usage se rapportant de façon raisonnable et directe à l'objectif premier pour lequel les renseignements ont été obtenus ou recueillis »[483].
Le SCT ajoute encore : « Cela signifie que les fins premières et les fins qui ont été proposées sont si intimement liées que la personne s'attendrait à ce que les renseignements soient utilisés pour les fins conformes, même si elles n'ont pas été expressément mentionnées »[484].

Nous pouvons observer une certaine évolution de cette notion dans la définition fournie par le SCT à cause de l'introduction d'un critère faisant référence aux « attentes » de la personne concernée.
Nous observons également que le SCT a voulu fournir une définition du « nouvel usage compatible » ou *new consistent use* en anglais, comme étant un « usage compatible n'ayant pas été présenté initialement dans la description appropriée des fichiers de renseignements personnels du chapitre de l'institution dans *Info Source* »[485].

---

[481] SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 332.
[482] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 325.
[483] *Id.*
[484] *Id.*
[485] *Id.*

En effet, le CPVPC affirme en 2006 que la notion d'usage compatible est, sans doute, l'une des notions les plus problématiques de la LPRP[486] et nous rappelle que, même si problème a été soulevé depuis plus de vingt ans – comme nous l'avons vu dans les lignes précédentes –, aucune amélioration n'a été apportée à cet égard, « sinon l'assurance que cette erreur ne serait pas répétée lors de l'élaboration de la LPRPDE »[487].

En effet, le législateur canadien a évité de reprendre cette notion dans la LPRPDE, applicable au secteur privé, et la notion des « fins acceptables », *appropriate purposes* en anglais, est celle qui a été utilisée.
Le paragraphe 5(3) de la LPRPDE dispose que « l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances ».
Nous constatons alors l'introduction d'une notion faisant référence directe au concept des « fins », plus proche du principe de finalité présent dans le droit européen, mais qui ne fonctionne pas par elle seule et doit être appréhendée à l'aide d'autres critères. Le législateur canadien a voulu offrir à l'interprète de la loi des éléments aidant à déterminer quels sont en effet les « fins acceptables » par des critères tels que celui de la « personne raisonnable » et « l'acceptabilité dans les circonstances ».

En 2004, la Cour fédérale révèle quelle est la volonté du Parlement canadien à l'heure d'approuver la LPRPDE : « L'objet consiste à fixer des règles régissant la collecte, l'utilisation et la communication des renseignements personnels d'une manière qui tienne compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances »[488]. En

[486] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 324, p. 30.
[487] *Id.*
[488] *Eastmond c. Canadian Pacific Railway*, (2004) C.F. 852 (nous soulignons).

effet, il y a à l'origine de la LPRPDE une certaine recherche d'équilibre et, dans cette équation, les attentes raisonnables dans la détermination des fins motivant la cueillette, l'utilisation et le transfert des renseignements personnels jouent un rôle de grande importance.

La jurisprudence de *Cheskes c. Ontario*[489], aussi appelée la « décision de la Loi sur l'adoption »[490], déclare inconstitutionnelles certaines des dispositions de ce texte de loi, qui auraient eu pour effet de permettre l'accès aux dossiers des parents biologiques ayant été scellés dans le passé en vue de garder leur confidentialité.

Cette décision est importante, comme certains l'ont fait remarquer, parce que le juge Belobaba a affirmé que la vie privée est devenu un « principe de justice fondamental »[491]. Le juge a même proposé une formule pour ce principe : *« Where an individual has a reasonable expectation of privacy in personal and confidential information, that information may not be disclosed to third parties without his or her consent* »[492].

La notion de « l'attente raisonnable » se trouve au centre de ce principe, ce qui accorde à une telle notion une grande importance à l'heure de déterminer si certaines informations peuvent être transférées à des tiers.
De plus, le juge renforce l'importance du droit à la vie privée dans l'actualité sur base de l'élément des « attentes raisonnables » et sur celui du droit de chaque personne à contrôler la circulation de l'information le concernant : « *Indeed, the two elements of the Suggested principle-the protection or reasonable expectations of privacy and the right of the individual to control the dissemination of his or her*

[489] *Cheskes c. Ontario* (Procureur général), (2007). O.J. Nº 3515.
[490] Voir à cet effet : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Équilibre entre protection de la vie privée et circulation de l'information*, Allocution présentée par Patricia KOSSEIM dans le cadre du Forum organisé par le *Population Therapeutics Research Group*, St. John's, Terre-Neuve-et-Labrador, novembre 2007.
[491] *Id.*
[492] *Cheskes c. Ontario* (Procureur général), (2007). O.J. Nº 3515 (nous soulignons).

*personal information-provide the bedrock for the modern understanding of privacy protection* »[493].

La jurisprudence de la Cour d'appel fédérale fournit une explication très claire au pourquoi de l'utilisation dans la LPRPDE de l'expression faisant référence aux « fins qu'une personne raisonnable estimerait acceptables dans les circonstances » :

> « Il y a donc deux intérêts concurrents dans l'objet de la LPRPDE : le droit de la personne à la vie privée d'une part, et le besoin commercial d'accès aux renseignements personnels d'autre part. Cependant, il y est expressément reconnu – par l'emploi des termes "à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances", qui sont repris au paragraphe 5(3) – que le droit à la vie privée n'est pas absolu. »[494]

Nous ne pouvons pas oublier que la notion des « attentes raisonnables » ou que le test de la « personne raisonnable » font partie intégrante de la construction du droit à la protection de la vie privée au Canada, et cela à partir de la Charte canadienne des droits et libertés[495]. Cela nous montre que cette notion est reliée de façon plus générale au droit à la protection de la vie privée au Canada, et non uniquement à la protection des renseignements personnels.

La Cour suprême du Canada a reconnu le statut de droit constitutionnel quand il a interprété la garantie prévue à la section 8 de la Charte canadienne des droits et libertés qui établit que « nul ne peut pénétrer chez autrui ni y prendre quoi que ce soit sans son consentement exprès ou tacite », comme protégeant la vie privée[496].
Il est important pour nous de souligner qu'aux États-Unis, la « *privacy* » tire son origine d'un principe équivalent, ce qui montre à nouveau une certaine proximité

---

[493] *Id.*
[494] *Englander c. Telus Communications*, (2004) F.C.A. 387.
[495] Charte canadienne des droits et libertés, partie I de la *Loi constitutionnelle de 1982*, [annexe B de la *Loi de 1982 sur le Canada*, c. 11 (R.-U.)] . (ci-après : Charte canadienne des droits et libertés).
[496] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997, p. 11-23.
Les auteurs soulignent l'importance de l'affaire *La Reine c. Dyment, [1988] 2 R.C.S. 417* dans la reconnaissance de la nature constitutionnelle du droit à la protection de la vie privée.

entre la construction du droit à la protection de la vie privée dans ces deux pays. J.Q. Withman souligne l'origine de ce droit aux États-Unis : « *In particular, "privacy" begins with the Fourth Amendment : At its origin, the right to privacy is the right against unlawful searches and seizures* »[497].
A. Levin et M.J. Nicholson mettent en exergue le fait que l'encadrement du droit à la vie privée que nous retrouvons dans la Charte canadienne des droits et libertés et celui que nous observons dans le 4e Amendement américain renferment des très grandes similitudes[498].

Même si la Charte canadienne des droits et libertés ne contient aucune mention explicite au droit à la protection de la vie privée, certains auteurs soulignent le rôle de la jurisprudence dans la délimitation d'un tel droit et l'importance des « attentes raisonnables » : « *The Canadian Charter of Rights and Freedoms contains no specific provisions concerning protection of privacy, but judgments and court decisions have consecrated the principle of privacy protection in accordance with reasonnable expectations* »[499]. Nous constatons alors qu'au Canada ces « attentes raisonnables » sont à l'origine de ce droit, de la même façon qu'aux États-Unis cette notion est indispensable dans l'interprétation du droit à la vie privée par les tribunaux : «*(…) This is particularly true when courts apply the "reasonnable expectation of privacy"test developed in the Fourth Amendement context* »[500].

Ce test de la « personne raisonnable », ou des « *reasonable expectations* » nous montre que, dans le droit canadien, ce critère du « raisonnable » va délimiter la protection accordée par le droit à la vie privée. Ainsi, certains auteurs nous rappellent l'idée suivante : « *not all aspects of privacy are protected, only those for which protection can reasonably be expected* »[501]. Ces expectatives raisonnables vont dépendre de plusieurs facteurs, mais un degré d'objectivité est exigé afin de

[497] J. Q. WITHMAN, préc., note 245, 1212.
[498] A. LEVIN et M. J. NICHOLSON, préc., note 245, 378.
[499] Pierre TRUDEL et France ABRAN, *Analysis of the Adequacy of Personal Data Protection in Canada, Report presented at the request of the European Commission, Justice and Home Affairs DG*, 2005, p. 13.
[500] J. Q. WITHMAN, préc., note 245, 1194.
[501] P. TRUDEL et F. ABRAN, préc., note 499 (nous soulignons).

bien cerner les contours d'un tel test. Voici comment ce test doit être réalisé dans la pratique :

> « *Assessment of the reasonableness of expectations wil of course depends on the context and nature of the information in question, where it is located, the purpose and circumstances of the rights violation, etc. The assessment cannot be subjective, but must be based on what a reasonable person placed in a similar situation would think, according to the decision of a lower court. The Supreme Court has rather insisted on taking into account all relevant factors, including subjective expectations about privacy and the reasonableness of such subjective expectations.* »[502]

La Cour suprême du Canada nous rappelle dans l'arrêt *R.c. 0'Connor*[503] le caractère non absolu de la protection de la vie privée qui doit « être pondérée en tenant compte des besoins légitimes de la société ».
La Cour nous rappelle que ce processus de pondération, repose essentiellement sur l'évaluation de « l'attente raisonnable » en matière de protection de la vie privée et la « pondération de cette attente » en regard de la nécessité de l'intervention de l'État.

Voici ce que la Cour expose à cet effet et qui place les « attentes raisonnables » au centre du dispositif devant servir à décider des possibles limitations au droit à la vie privée au Canada : « Évidemment, plus l'attente raisonnable en matière de protection de la vie privée sera grande et plus les effets préjudiciables découlant de sa violation seront importants, plus l'objectif de l'État ainsi que les effets bénéfiques de cet objectif devront être impératifs afin de justifier toute entrave à ce droit ».

Ce critère est utilisé dans d'autres pays, comme en Belgique où le législateur énonce également le principe fondamental de finalité à l'article 4 de la Loi belge en la matière[504], en ajoutant également des précisions sur le « problème fondamental

---

[502] *Id.*, p. 15 et 16.
[503] *R. C. O'Connor*, (1995), 4 R.C.S.
[504] *Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*.

de la réutilisation ultérieure des données »[505]. En effet, le législateur belge, tout comme le législateur canadien dans le cadre du secteur privé, utilise le critère des « prévisions raisonnables de l'intéressé », comme instrument déterminant pour éviter que les données personnelles soient traitées ultérieurement de manière incompatible avec les finalités de départ.

Ainsi, le texte belge dispose que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu du fait que tous les facteurs pertinents, notamment les prévisions raisonnables de l'intéressé et les dispositions légales et réglementaires applicables[506].

Le législateur belge offre un éventail de critères pour déterminer les usages compatibles des données, puisqu'il n'existe pas de critère absolu[507], si bien que celui des « prévisions raisonnables de l'intéressé » reste déterminant.
Le CPVPC établit des critères très clairs dans l'éventualité que la notion « d'usage compatible » soit conservée dans la LPRPDE et note également que, dans ces circonstances, elle devrait être définie de manière claire et limitée.

Ainsi, le CPVPC établit d'une part, que l'« usage compatible » dans le cadre du mandat général d'une institution gouvernementale « ne constitue pas une justification suffisante et, en aucun cas, on ne peut faire appel au couplage de données sous prétexte qu'il constitue un usage compatible »[508].

Voilà la première des règles que le CPVPC pose pour la détermination d'un « usage compatible », ne devant pas pouvoir faire appel à la technique du couplage pour justifier certains usages.

---

[505] Thibault VERBIEST et Étienne WÉRY, *Le droit de l'Internet et de la société de l'information, Droits européen, belge et français*, De Boeck et Lancier, Bruxelles, 2001, p. 435.
[506] Alinéa 4(1)2) de la *Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*.
[507] T. VERBIEST et É. WÉRY, préc., note 505, p. 435.
[508] COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 324, p. 30.

D'autre part, étant donné que l'utilisation proposée doit être compatible avec la fin pour laquelle les renseignements ont été recueillis et que cette fin doit avoir un lien direct avec un de leurs programmes ou une de leurs activités spécifiques, le CPVP établit une règle à suivre. Pour le CPVPC « c'est le programme ou l'activité qui sert de point de référence pour déterminer si une utilisation donnée de renseignements personnels répond à la notion "d'usage compatible" et non le mandat général de l'institution »[509].

Ainsi, nous observons que la mission ou le mandat général de l'institution gouvernementale ne peut pas servir par elle seule à justifier n'importe quel usage et que c'est notamment par rapport à l'activité qu'il faut déterminer si une utilisation est compatible.

Finalement, le CPVPC souligne l'importance de la vérification du critère de « lien raisonnable et direct » qui doit être effectuée lors d'un « usage compatible » des renseignements personnels.

Le SCT établit certains critères essentiels de violation de la vie privée devant être interreliés afin de déterminer si la divulgation d'un renseignement pourrait porter atteinte à la vie privée.
Ces critères ont été dégagés par le SCT afin d'apprécier si les conditions que le sous-alinéa 8(2)m) (i) établit se retrouvent et ainsi appliquer cette exception au régime général. Cette disposition fait référence aux cas où un intérêt public justifierait nettement une éventuelle violation de la vie privée.
Cette disposition concerne la communication de renseignements personnels dans des situations imprévisibles et exceptionnelles. Selon le SCT et dans tous les cas, ce sous-alinéa ne doit être utilisé que « de manière très restrictive et les renseignements ne devraient être divulgués en vertu de cette disposition que

[509] *Id.*

lorsqu'il est évident que l'intérêt public le commande et que cette situation ne tombe pas sous le coup d'un autre alinéa du paragraphe 8(2) »[510].

Mais, comme le SCT nous le rappelle, il n'y a pas de formule toute faite pour déterminer où réside le véritable intérêt du public et, dans la plupart des cas, l'intérêt public ne saute pas aux yeux, raison pour laquelle l'utilisation des trois critères mentionnés s'impose.

Le premier des critères fait référence aux « attentes de l'individu » devant être examinées d'une part, les conditions ayant régi la collecte des renseignements personnels. Pour cela, il faut vérifier si les renseignements ont été recueillis selon des termes interdisant la divulgation sous une forme quelconque.

D'autre part, en examinant les attentes de l'individu, il faut analyser s'il s'agit de renseignements non sollicités ou donnés librement par un individu qui ne s'attend pas à ce qu'ils soient gardés confidentiels. Il est essentiel également de regarder si l'individu a rendu publics ces renseignements, en abandonnant ainsi son droit à la protection de sa vie privée.

Le deuxième critère se base sur la « nature délicate des renseignements », selon lequel il faut examiner s'il s'agit de renseignements de nature plutôt délicate ou plutôt anodins et s'ils sont très actuels ou si au contraire, en raison du temps écoulé, le degré de sensibilité a diminué.

Finalement, comme troisième critère, il s'agit d'analyser la « probabilité d'un préjudice » mesurable dans le cas de divulgation de renseignements jugés de nature délicate. Le SCT signale plus concrètement le besoin de vérifier si une telle divulgation pourrait entraîner notamment une atteinte au bien-être, à la réputation et à la sécurité de l'individu.

[510] SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA, préc., note 332.

Mais il faudra également que le responsable de l'institution évalue si les renseignements ainsi communiqués peuvent permettre à une autre institution fédérale de prendre des décisions qui n'ont rien à voir avec les motifs pour lesquels la demande de communication a été présentée[511].
Nous constatons que ces trois critères constituent un outil précieux, pouvant être utilisé en général avant de procéder à la communication de renseignements personnels à des tiers.

Le professeur Benyekhlef fait remarquer que l'énonciation de ces guides du SCT est méritoire, toutefois il regrette que la loi ne prévoit rien à ce sujet[512].
En effet, cet auteur nous rappelle que la violation de ces directives par le responsable de l'institution n'entraîne aucune conséquence légale et l'erreur dans l'interprétation de celles-ci mène au même résultat.
Il convient donc de retenir que : « Cette absence de sanction amoindrit l'intérêt de ces directives et laisse entier le problème de la trop grande discrétion accordée au responsable de l'institution détentrice des renseignements personnels »[513].

**2- Le couplage des données dans le secteur public canadien**

La question relative au « couplage des données » dans le secteur public canadien, ainsi que le besoin d'encadrer une telle pratique sont des thèmes touchant à l'adéquation de la LPRP aujourd'hui.

Dès en 1987, cette notion a été définie comme étant un processus d'interconnexion de fichiers ou de comparaison de renseignements personnels comme ce qui suit : « comparaison de listes ou de fichiers différents pour déterminer si des renseignements identiques, similaires ou contradictoires y apparaissent »[514].

---

[511] *Id.*
Voir les trois critères avancés par le SCT dans ce document.
[512] K. BENYEKHLEF, préc., note 313, p. 125.
[513] *Id.*
[514] STANDING COMITTEE ON JUSTICE AND SOLLICITOR GENERAL ON THE REVIEW OF THE ACCESS TO INFORMATION ACT AND THE PRIVACY ACT, préc., note 468, p. 51.

Ceux qui définissent ainsi cette notion soulignent également que les noms, les numéros d'assurance sociale, les adresses ou d'autres données personnelles peuvent être utilisés.

Nous constatons alors que le terme « couplage » est utilisé pour désigner l'opération que, dans le contexte européen, nous reconnaissons comme une « interconnexion » et qui est intimement reliée au principe de finalité.

C'est dans le contexte du premier examen à la LPRP en 1987, que des experts affirment que la LPRP ne traite pas de la question du couplage ou de l'interconnexion « en termes aussi explicites qu'il le faudrait, même si elle établit à l'article 7 le principe fondamental selon lequel les renseignements personnels ne peuvent servir qu'aux fins auxquelles ils ont été recueillis »[515].

De plus, pour certains, puisque l'interconnexion des ordinateurs suppose la comparaison de renseignements recueillis à des fins différentes, la pratique en question est contraire au paragraphe 7(a) de la LPRP interdisant une utilisation des renseignements autre qu'aux fins pour lesquelles ils ont été recueillis, de même que pour des usages compatibles à ces fins[516].

Il est clair, dès ce moment, que les articles 7 et 8 de la LPRP ne sont pas capables d'encadrer les techniques de couplage et les experts recommandent « d'interdire expressément le couplage de données s'il suppose l'utilisation des données à des fins incompatibles avec les fins auxquelles elles ont été recueillies à l'origine »[517].
Cette technique de l'interconnexion a suscité dans le contexte canadien des craintes équivalentes à celles ayant été au centre du débat en Europe.
Le Comité ayant réalisé le rapport suite au premier examen de la LPRP a expressément recommandé que ce texte interdise le couplage des données, sauf dans certains circonstances et, très particulièrement, lorsqu'il s'agit de couplages

[515] *Id.*, p. 52.
[516] *Id.*
[517] *Id.*

supposant l'usage de données personnelles relevant d'une autre institution gouvernementale[518].

En effet, « c'est justement ce lien, cette agrégation de renseignements personnels, qui, de l'avis de plusieurs, constitue l'une des plus grandes menaces courantes en matière de protection des droits à la vie privée »[519].

Cette recommandation a eu pour résultat des règles qui ont pris la forme d'une politique du SCT sur le couplage de données en 1989[520], politique qui a été revue pour la dernière fois en 1993 et qui a été remplacée par une directive en 2008. Cette politique impose des obligations pour les organisations du secteur public canadien, notamment la tenue d'un examen préliminaire de la faisabilité d'un programme de couplage ou *data matching*.

Cette évaluation comporte certaines étapes, entre autres l'analyse des avantages du programme de couplage par rapport à d'autres méthodes de contrôle, de gestion ou d'application de la Loi.

Il est également nécessaire de vérifier si les renseignements personnels que veut recueillir une institution fédérale présentent un lien direct avec ses programmes ou ses activités, afin de respecter les conditions que la LPRP impose.

Il est également important, selon cette politique du SCT, « de vérifier s'il est possible de recueillir auprès de l'individu lui-même les renseignements personnels le concernant ou si la collecte par couplage de données peut être autorisée parce que l'une ou l'autre des conditions suivantes existe : l'individu autorise la collecte indirecte, l'institution pourrait obtenir les renseignements d'une autre source sans aucun consentement aux termes du paragraphe 8(2) de la LPRP, ou la collecte faite directement pourrait avoir pour résultat la collecte de renseignements inexacts ou

---

[518] *Id.*, Recommandation nº 5.7.

[519] Heather BLACK, *Réforme des lois sur la protection des renseignements personnels et de la vie privée : Réponse à un monde en réseau*, Allocution présentée dans la Série Conférenciers invités McCarthy Tétrault, Halifax (Nouvelle-Écosse), 3 février 2005.

[520] Voir à ce sujet : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 324, p. 32.

contrarier les fins ou compromettre l'usage auquel les renseignements sont destinés »[521].

Mais cette évaluation impose également de « déterminer s'il est nécessaire d'avertir la personne en cause du nouvel usage fait des renseignements personnels la concernant et des modalités suggérées à cet effet, ou les raisons pour lesquelles il n'est pas nécessaire d'informer la personne concernée ».

En effet, les nouveaux usages qui peuvent être faits des renseignements personnels présentent des risques pour le droit à la protection des renseignements personnels, pouvant causer des préjudices aux citoyens. La possibilité d'être informés et la transparence des nouveaux usages des renseignements personnels sont dès lors cruciales afin de contrebalancer ce potentiel de risque. Toutefois, nous avons pu observer la grande marge qui existe en ce qui concerne le fait de décider d'informer la personne concernée, ce qui prouve la possibilité de détourner cette mesure assez facilement.

Le SCT recommande également l'analyse de coûts et avantages des projets de couplage des données, comportant l'évaluation des différents facteurs visant à déterminer s'il convient d'aller de l'avant avec le programme de couplage.

Notons que dans le modèle d'évaluation des facteurs relatifs à la vie privée[522], EFVP, élaboré par le SCT en 2002[523], on a demandé aux ministères s'ils faisaient du couplage de données, ce qui montre l'importance accordée à ce phénomène lors de l'évaluation des risques potentiels pour ce qui est de la protection des renseignements personnels au sein d'une institution.

Le CPVPC souligne qu'il est difficile de savoir si le couplage des données va inclure uniquement le couplage traditionnel des données ou s'il comporte également la liaison de données, le profilage et le forage de données. Est important

[521] SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Politique sur le couplage des données*, 1989.
[522] Ci-après : ÉFVP.
[523] SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Politique d'évaluation des facteurs relatifs à la vie privée*, 2002, en ligne : "http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12450" (consulté le 11 février 2011).

aussi le fait qu'il n'existe pas de distinction claire entre « le couplage des données à des fins administratives et celui qui est fait à des fins non administratives »[524].
Le CPVPC souligne en 2005 que tous les Commissariats existant dans les provinces canadiennes ont fait la recommandation d'apporter des modifications à la LPRP afin de s'assurer que les institutions gouvernementales relient les dossiers personnels dans des systèmes discrets uniquement lorsqu'il est possible d'en démontrer la nécessité, et tout cela sous la surveillance permanente et vigilante du CPVPC[525].

Il faut noter que ces recommandations n'ont pas été exécutées. De plus, compte tenu du peu de propositions de couplage de données qu'a reçues le CPVPC ces dernières années et compte tenu que la pratique est vraisemblablement répandue, il est grand temps de prévoir des obligations à cet effet dans la Loi[526].

En 2000, la Cour d'appel fédérale a rendu une décision[527] montrant très clairement le manque d'utilité de certaines dispositions de la LPRP à l'heure de contrôler la communication continue des renseignements personnels recueillis à une seule fin et utilisés pour des activités de couplage pour des usages complètement différents.

Plus concrètement, la Cour affirme que « la vaste gamme d'exceptions permises par le paragraphe 8(2) (de la LPRP) témoigne incontestablement de l'intention du législateur de permettre la communication de renseignements personnels à des personnes qui n'ont absolument aucun lien avec les institutions qui les communique et pour des fins autres que celles pour lesquelles ces renseignements ont été recueillis »[528].

---

[524] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 324, p. 32.
[525] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 470, p. 26.
[526] *Id.*
[527] *Loi sur la protection des renseignements personnels (Can.) (Re), (2000) 3 C.F. 82.*
[528] *Id.*

La Cour affirme également que :

> « on ne peut pas faire autrement que d'interpréter l'alinéa 8(2)b) comme étant une disposition permettant au législateur de conférer à tout ministre (par exemple), au moyen d'une loi donnée, un large pouvoir discrétionnaire quant à la forme et au fond relativement à la communication de renseignements personnels que son ministère a recueillis, ce pouvoir discrétionnaire devant naturellement être exercé conformément à l'objet de la LPRP (...) Mais on ne peut tout simplement pas conclure, à partir de l'omission du législateur d'être précis à l'alinéa 8(2)b) alors qu'il désirait manifestement s'exprimer en termes généraux, que cet alinéa ne permet pas à une institution fédérale de communiquer à une autre institution fédérale des renseignements personnels qu'en l'absence d'interdiction expresse, elle peut communiquer à des institutions étrangères. »[529]

Il faut dire que, en 2001, la Cour suprême du Canada[530] a confirmé la décision de la Cour fédérale. Il est clair que la jurisprudence souligne et confirme la grande marge que certaines dispositions de la LPRP offrent aux institutions fédérales canadiennes pour communiquer des renseignements personnels à des tiers.

Nous devons souligner également que, dans pareil contexte, il semble de plus en plus nécessaire de pouvoir avoir recours à des mécanismes capables d'aider les institutions fédérales à gérer les risques pouvant dériver du couplages des données ou des communications entre institutions du secteur public canadien.

Pour ce qui est du couplage des données ou de l'échange de données entre organismes du secteur public, il nous semble que les ÉFVP peuvent constituer un outil aidant à compléter le cadre offert par la LPRP sur ces questions. En effet, l'obligation de procéder à ces ÉFVP peut servir à apporter une réponse à la LPRP, très silencieuse sur le sujet des interconnexions et du couplage des renseignements dans le secteur public. Nous étudierons dans les pages qui suivent comment ces évaluations se réalisent au Canada dans le contexte du secteur public.

---

[529] *Id.*
[530] *Loi sur la protection des renseignements personnels (Can.) (Re), (2001) 3 R.C.S. 905.*

Le CPVPC dans son Rapport 2006-2007 nous rappelle que la LPRP ne contient aucune règle de base sur le couplage de données, y compris le forage et l'agrégation de données[531]. Le CPVP a demandé à cette occasion que la LPRP soit réformée, notamment afin de définir les principes devant guider le couplage de données et les responsabilités des parties concernées. De plus, le CPVPC a souligné que la loi devrait exiger des institutions fédérales qu'elles obtiennent l'approbation du CPVPC avant de procéder à la mise en place des initiatives de couplage.

Bien sûr, le CPVPC a également affirmé en 2007 que le CPVPC devait avoir le pouvoir de faire cesser les activités de couplage de données si cela pouvait entraîner des risques dans le domaine de la protection de la vie privée[532].

Aujourd'hui, le législateur n'a pas encore donné force de loi à la directive sur les ÉFVP, qui sans doute pourrait contribuer à rendre plus transparentes les communications entre les organismes.

De plus, le CPVPC n'a pas le pouvoir de faire cesser les activités de couplage ou la communication de renseignements entre organismes si celle-ci ne satisfait pas aux normes établies. Il faudra donc examiner si ces outils de gestion de la protection des renseignements personnels pourront être efficaces dans le futur, même si le pouvoir du CPVPC se limite à donner des conseils en la matière et qu'il ne lui est pas possible pour l'instant de rendre des ordonnances.

Certains nous rappellent quelle sont les limitations du CPVPC à cet effet : « si, en revanche, une organisation a indûment communiqué des renseignements personnels, ce qui va à l'encontre de la Loi sur la protection des renseignements personnels, notre seul recours est de formuler des recommandations à l'intention de l'institution gouvernementale pour qu'elle modifie ses pratiques »[533].

---

[531] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2006-2007 concernant la Loi sur la protection des renseignements personnels*, 2007, p. 10.

[532] *Id.*

[533] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Leçons tirées du secteur public*, Commentaires présentés par Chantal BERNIER dans le cadre d'un débat d'experts lors de la Conférence du groupe *Access Privacy*, le 25 mars 2010, Toronto, Ontario.

La question entourant le couplage de données dans le contexte canadien représente sans aucun doute un des enjeux les plus importants dans le contexte de la notion de la finalité des renseignements personnels.

## CHAPITRE 2 PRINCIPE DE FINALITÉ, STANDARDS JURIDIQUES ET PONDÉRATION DES INTÊRÉTS

Nous verrons dans les lignes qui suivent que la technique du standard juridique est facilement identifiable dans les lois, la jurisprudence et les décisions des autorités de contrôle quand il s'agit d'encadrer la protection des renseignements personnels. En effet, il est essentiel, dans le cadre de nos recherches, de nous pencher sur la question de l'utilisation des standards juridiques en matière de protection des renseignements personnels au Canada et en Europe. Le débat doctrinal entourant cette question ne peut pas nous empêcher d'identifier les particularités que les standards présentent dans ce domaine et d'essayer de comprendre un peu mieux quel est le rôle qu'ils jouent dans la protection de la vie privée.

Par la suite, nous tenterons d'identifier quelle est la démarche entreprise par les autorités de contrôle afin de comprendre mieux encore comment ont été délimités les contours du principe de finalité. L'étude de dossiers, qui a été réalisé au sein de la CNIL et du CPVPC, nous montrera encore la présence de standards dans ce domaine et surtout nous guidera dans l'étude de la mise en œuvre de la technique de la pondération des intérêts en jeu dans le cadre des dossiers en la matière.

Le principe de finalité et celui de proportionnalité se trouvent au centre de ce dispositif ayant pour but de trouver l'équilibre recherché dans ces dossiers. Nous observerons que la nature des standards sera également opérationnel dans le contexte de l'administration électronique où les principes de protection de la vie privée sont appelés à jouer un rôle essentiel.

## SECTION 1 Droit à la protection des renseignements personnels et la technique du standard

Nous avons étudié dans les pages précédentes les articles de loi faisant référence à la notion de finalité dans le contexte de la protection des renseignements personnels se trouvant dans les textes européens et canadiens. Nous avons analysé également d'autres dispositions ayant un rapport avec ce principe et pouvant nous éclairer dans la détermination de ses contours.

De même, nous avons étudié la doctrine afin de comprendre encore mieux comment le principe de finalité a été appréhendé des deux côtés de l'Atlantique par les experts et interprètes des textes en la matière.

À partir du début de l'étude sur « l'historique » que nous avons voulu tracer du principe de finalité, puis plus tard en analysant le travail des autorités de contrôle et du juge, nous avons pu observer une tendance qui se répète dans le temps, tant en Europe qu'au Canada.

En effet, nous observons une caractéristique se trouvant dans la formulation des dispositions canadiennes et européennes, à caractère national, international ou communautaire, faisant référence au principe de finalité et dans la législation en matière de protection des renseignements personnels en général, qui mérite notre étude.

Nous avons déjà évoqué à plusieurs reprises le fait que les contours du principe de finalité sont plutôt flous et nous avons analysé les dispositions relatives à ce principe. C'est seulement après une telle analyse que nous arrivons à un constat qui mérite toute notre attention. En effet, ce que nous observons quand nous analysons comment le législateur a voulu encadrer ce critère de la finalité dans les dispositions en question, c'est le recours qui a été fait très souvent à ce que la doctrine qualifie de technique du « standard » juridique.

Nous observons cette tendance dans une multitude de dispositions et de textes en la matière, ce qui nous permet de comprendre que le droit relatif à la protection des renseignements personnels comporte très souvent l'utilisation de ce type de technique. Il s'agit d'un recours auquel le législateur a souvent fait appel dans l'élaboration des textes régissant cette matière et que nous constatons par une grande présence de standards juridiques dans ce domaine.

D. Kewer souligne l'importance des standards dans le contexte actuel en affirmant que « *standards globally proliferate because they are more compatible with regulatory autonomy of states than binding directives* »[534].

Bien sûr, la question de l'utilisation de la technique du standard dans le droit relatif à la protection des renseignements personnels, pourrait faire l'objet d'une recherche consacrée exclusivement à ce sujet. Dans le cadre de nos travaux, nous allons faire référence à cette question afin de comprendre encore mieux comment fonctionne dans la pratique l'application du principe de finalité.

Il nous semble d'une grande importance de procéder ou pour le moins d'aborder la question de l'utilisation des standards dans le droit relatif à la protection des renseignements personnels, sans faire nécessairement une analyse approfondie de la question.

Il s'agira donc de toucher à la question sans vouloir nécessairement classifier les différentes notions à étudier comme des « standards » ou des « notions à contenu variable » et sans avoir pour objectif leur catégorisation ; et donc exclusivement de montrer comment ces notions fonctionnent ainsi que de les identifier dans les lois et dans le travail qui est fait par les interprètes des lois.

Pour cela, nous identifierons dans un premier temps la manière dont cette tendance se présente dans les textes de loi.

Plus tard, il sera question d'identifier ces notions dans le travail que les interprètes de la loi, notamment les autorités de contrôle, ont réalisé par le passé dans les

---

[534] Dieter KERWER, "Rules that Many Use : Standards and Global Regulation", *Governance : An International Journal of Policy, Administration and Institutions*, Vol. 18, No. 4, 2005, en ligne : http://onlinelibrary.wiley.com/doi/10.1111/j.1468-0491.2005.00294.x/abstract (consulté le 6 juillet 2010)

délibérations et avis donnant lieu à une jurisprudence et à une doctrine qui ont défini le critère de finalité.

Il s'agira finalement d'analyser ce que nous pouvons qualifier de « données brutes » relatives aux dossiers d'enquête et aux plaintes des citoyens, afin de déterminer comment cette tendance est observable dans le travail réalisé par les autorités de contrôle dans le processus visant à adopter une décision dans les cas où le principe de finalité se trouve au centre du débat.

Nombreux sont les auteurs qui ont traité le thème des standards en droit, il sera important pour nous de faire ressortir quelques points importants de ces théories afin d'établir sous quel point de vue nous avons envisagé de réaliser notre analyse à travers de l'étude du droit relatif à la protection des renseignements personnels.

Il s'agira uniquement d'un petit survol de la question pour essayer plus tard d'identifier les standards utilisés dans les dispositions relatives au principe de finalité.

**1- Protection des renseignements personnels, standards et notions à contenu variable : quelques précisions et débat doctrinal**

La question du standard juridique présente une grande complexité que nous pouvons observer en analysant la doctrine en la matière. Le débat autour de cette notion porte sur sa nature et sa définition mais également sur des questions terminologiques qui ont été à l'origine des théories portant sur la spécificité du standard ainsi que sur la volonté d'arriver à une catégorisation des standards et des notions à contenu variable.

M. O. Stati nous rappelle qu'on exige au Droit deux qualités essentiellement contradictoires : d'une part, le Droit doit être ferme et rigide afin de remplir sa fonction sociale qui est celle d'assurer l'ordre et la paix dans la sécurité et rendre la vie sociale possible ; d'autre part, le Droit doit faire preuve d'une certaine

souplesse, « à côté d'une certaine rigidité »[535], afin de régir les rapports économiques et sociaux et de s'y adapter.
Cet auteur se demande comment trancher le conflit entre ces deux exigences et, dès 1927, avance que le standard juridique pourrait contribuer dans une certaine mesure à donner une solution plus heureuse au problème[536].
En effet, pour cet auteur, « il n'y a pas de procédé plus particulièrement favorable à l'évolution du Droit et qui se prête mieux à son adaptation continuelle aux conditions perpétuellement changeantes du milieu social, que cet instrument »[537].

*A priori*, à cause des particularités du droit relatif à la protection des renseignements personnels, nous pouvons affirmer que ce procédé est spécialement capable de répondre adéquatement aux besoins concrets en la matière. Le droit relatif aux nouvelles technologies de l'information requiert une adaptation perpétuelle à une réalité toujours changeante et la technique du standard juridique semble pouvoir répondre à ce besoin de façon optimale.

La doctrine met particulièrement en relief le cas des textes législatifs « qui promulguent des principes rédigés dans une forme générale et imprécise à l'aide de termes abstraits et difficiles à définir et imposant des standards de la plus grande relativité »[538].

Nous assistons depuis quelques années à l'utilisation de la notion de « standard », ainsi que celle de « notion à contenu variable » pour faire référence à ce type de procédé, ce qui nous oblige à revenir sur ces concepts afin de pouvoir clarifier ces notions dans le cadre de notre étude.
Toutefois, il s'agira uniquement de comprendre si effectivement nous identifions des éléments pouvant nous montrer comment ce procédé fonctionne et,

[535] Marcel O. STATI, *Le Standard juridique*, Paris, Librairie de jurisprudence ancienne et moderne, 1927, p. 29.
[536] *Id.*
[537] *Id.*, p. 89.
[538] Diane L. DEMERS, « Les concepts flous, l'interprétation constructiviste et la modélisation », dans Claude THOMASSET et Danièle BOURCIER (dir.), *Interpréter le droit : le sens, l'interprète, la machine*, Bruxelles, Bruylant, 1997, 221, p. 234 (nous soulignons).

concrètement, quelles sont les implications d'une telle technique dans l'application du principe de finalité.

Dans le cadre de nos travaux seule nous intéresse la question de vérifier si des standards se trouvent dans la formulation et la délimitation du principe de finalité, sans vouloir vraiment se positionner dans le débat qui entoure la théorie relative aux standards.

C. Castets-Renard souligne que « le terme *standard* trouve ses origines en droit anglo-saxon, mais la doctrine semble préférer aujourd'hui le terme *notion à contenu variable* »[539].

S. Rials fait remarquer que dans une enquête réalisée sur les notions à contenu variable, il était vraiment difficile de ne pas rencontrer la notion de standard, même si elle n'est pas tellement utilisée de nos jours. Pour cet auteur, cet abandon est légitime à cause de l'utilisation qui a été parfois faite par la doctrine de cette notion, « qui l'a ensevelie sous un tel amas de vraies erreurs et de demi-vérités qu'elle l'a rendue inutilisable pour tout juriste de bon sens »[540].

Toutefois, pour lui, c'est justement grâce à toutes ces erreurs que la notion de standard va favoriser l'appréhension des tensions majeures de la matière juridique. Une des questions les plus complexes est celle qui touche à la distinction entre la nature du standard et celle de la règle, ainsi que celle du principe. Pour résumer cette opposition, A.A. Sanhoury avance que :

> « Le *standard*, directive générale et mesure de conduite, échappe, par sa nature souple et adaptable, d'une part, à la fixité rigide et à la précision inflexible qui rendent immuable la *règle*. Et, d'autre part, à l'abstraction logique et à la subjectivité excessive qui dénaturent le *principe* et le rendent peu adaptable. »[541]

---

[539] Céline CASTETS-RENARD, *Notions à contenu variable en droit d'auteur*, Paris, l'Harmattan, 2003, p. 19.

[540] Stéphane RIALS, "Les standards, notions critiques du droit", dans Ch. PERELMAN et R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Ch, Bruxelles, Bruylant, 1984, 39, p. 40.

[541] A.A. SANHOURY, *Les restrictions contractuelles à la liberté individuelle de travail dans la jurisprudence anglaise*, Paris, Marcel Giard , 1925, p. 44.

Dès lors, pour cet auteur, le « principe » se présente comme le résultat « d'une abstraction logique et d'une généralisation schématique fort éloignées de la réalité »[542], raisons pour lesquelles, le principe trouve mieux sa place dans les sciences mathématiques et les sciences naturelles.
Par contre, il affirme que le « standard » n'a rien d'abstrait, il se prête à une application pratique et immédiate et trouve sa place dans les sciences sociales, parce que dans les sciences sociales « on ne peut pas négliger les irrégularités qui existent en fait, sans risquer d'aboutir à des conceptions purement idéales et sans aucun rapport avec la réalité »[543].

R. Pound avait défini le standard comme étant une « mesure moyenne de conduite sociale correcte », et cela dans le cadre de la « Jurisprudence sociologique » qui opère à partir de quatre instruments de la technique : les règles, les principes, les conceptions et les standards[544]. Il faut souligner également que cette Jurisprudence sociologique se caractérise par la recherche d'un équilibre entre des intérêts économiques et sociaux parfois antagoniques, grâce à la technique du « *balancing of interest* ».

A.A. Sanhoury définit dans sa thèse de doctorat publiée en 1925 le standard comme étant une « directive générale destinée à guider le juge dans l'administration du droit et à lui donner une idée de son but et de sa finalité »[545]. Cet auteur affirme qu'à la différence de la règle, le standard ne lie pas étroitement le juge qui est libre de choisir le chemin pour arriver à un but déterminé.

Pour S. Rials, le standard est un « instrument de mesure »[546] et C. Perelman qualifie les standards comme des « critères fondés sur ce qui paraît normal et acceptable dans la société au moment où les faits doivent être appréciés »[547].

---

[542] *Id.*
[543] *Id.*
[544] Voir à ce sujet les publications de R. Pound, entre autres : R. POUND, « The Administrative Application of Legal Standards », *Reports of the American Bar Association*, vol. n. 44, 1919, 445.
[545] A. A. SANHOURY, préc., note 41, p. 23.
[546] S. RIALS, préc., note 540, p. 44.

M. O. Stati signale qu'il existe une contradiction initiale qui rend impossible une définition scientifique du standard juridique, et cela parce que le standard est essentiellement concret et foncièrement empirique. En conséquence, il ne saurait être conçu autrement que par rapport à certains éléments de fait ni déterminés ni défini *in abstracto* ni *a priori.*

Toutefois, si on essaie de définir le standard, cet auteur propose du point de vue de la technique moderne du droit cette définition : « procédé qui prescrit au juge de prendre en considération le type moyen de conduite sociale correcte pour la catégorie déterminée d'actes qu'il s'agit de juger »[548].

Pour P. Catala, les standards sont des modèles de comportement ou des situations types auxquels le juge est invité à se référer pour trancher une situation. Des plus, ces notions sous leur formulation objective ont un caractère de généralité abstraite et vont permettre au magistrat de qualifier le fait brut, puisque « ces standards sont des médias entre le fait brut et le droit »[549].

Pour cet auteur, le juge a un très fort pouvoir d'appréciation et « dans la durée ces standards sont plastiques »[550]. Dès lors, cet auteur souligne que l'inclusion de standards dans les dispositions de la loi conduit à un « droit flexible » et ménage la faculté d'adaptation de la norme.

De plus, il affirme que le standard réalise une « économie du détail » et donne l'exemple très illustrateur d'une loi devant établir le portrait-robot d'un bon père de famille et qui devrait nécessairement utiliser au moins une cinquantaine d'articles pour l'établir.

---

[547] Chaím PERELMAN, « Les notions à contenu variable, Essai de synthèse », dans Ch. PERELMAN et R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 363, 1984.

[548] M. O. STATI, préc., note 535, p. 45.

[549] Pierre CATALA, « Unité ou complexité », dans *Droit et informatique, L'hermine et la puce*, Coll. Fredrik R. Bull, Vol. 11, Paris, Masson, 1992, p. 14.

[550] *Id.*

E. Reidel voit les standard comme des « *tools of interpretation, and guidelines or yardsticks of reasoning for existing but open hard law rules and principles* »[551], dans le cadre de son travail sur les standards dans le contexte du droit international.

C. Castets-Renard, dans sa thèse de doctorat sur les notions à contenu variable en droit d'auteur, expose les résultats d'une recherche consacrée uniquement à l'étude de ces notions dans ce domaine du droit.

Elle affirme que les notions à contenu variable sont un instrument de souplesse normative et offrent au juge la possibilité d'établir une balance des intérêts au regard du contexte social et du cas d'espèce.
En effet, si la souplesse normative est privilégiée, l'utilisation des notions à contenu variable est opportune, puisqu'elle va « éviter de légiférer à chaque mutation technique, tant au niveau national que communautaire ou international »[552].
Raison pour laquelle, l'étude des notions à contenu variable dans le cadre du droit d'auteur peut servir à apporter des connaissances importantes en la matière.
L'étude de ces notions dans le cadre du droit relatif à la protection des renseignements personnels nous semble également pertinente et évidente à cause des caractéristiques propres à ce domaine.
Certains auteurs tels que A.A. Al-Sanhoury affirment que « les standards ne visent pas des faits précis, mais donnent une mesure moyenne de conduite sociale correcte dans les domaines mouvants du droit »[553], ce qui démontre également que l'étude de ces notions dans le cadre de la protection des renseignements personnels, domaine juridique essentiellement « mouvant », devient tout à fait naturelle.

Selon C. Castets-Renard, il est clair que les notions à contenu variable englobent les standards et les notions cadre et elle dénonce un problème majeur venant du fait

[551] Eibe REIDEL, « Standards and Sources. Farewell to the Exclusivity of the Sources Triad in International Law? ", (1991) 2 EJIL, 58, 83.
[552] C. CASTETS-RENARD, préc., note 539, p. 12.
[553] A. A. SANHOURY, préc., note 541, p. 31.

que toutes les notions sont très souvent mêlées et confondues, même si certaines d'entre elles sont plus restrictives et doivent être différenciées[554].

Pour cette auteure, la doctrine a différencié des notions, alors même qu'elles renvoient à une même réalité conceptuelle et, à l'inverse, des concepts différents ont été désignés par des expressions identiques.
Ainsi, afin de cerner l'objet de l'étude des notions à contenu variable, elle réalise une analyse terminologique et propose une définition de la notion à contenu variable : « notion dont le signifiant, le contenant reste fixe alors que le signifié, le contenu, évolue dans le temps et dans l'espace »[555].
Ces notions à contenu variable se caractérisent alors par le fait que le signifiant est stable et le signifié est évolutif, puisqu'il est adapté par le juge à chaque cas.
R. Legros affirme également que la notion à contenu variable est une « notion dont la dénomination, le signifiant, restent constants, mais dont le domaine, le champ, le signifié sont mouvants, évoluent, plus spécialement en fonction de facteurs spatio-temporels »[556].

J. Carbonnier parle de « variabilité », et non d'un mouvement constaté en fait, plutôt de « l'aptitude en droit à se mouvoir, une disponibilité de certaines notions juridiques, leur ouverture au changement »[557], qui a été voulue par le législateur. Toutefois, cet auteur va encore plus loin dans son analyse et parle, d'une part, d'une variabilité préparée d'avance, d'une certaine intentionnalité inhérente à la variabilité et qui est fondamentalement une technique législative ; et, d'autre part, il oppose nettement une « variabilité *ex post facto* » qui se produit par une action imprévue de la part des interprètes[558].

---

[554] C. CASTETS-RENARD, préc., note 539, p. 23.
[555] *Id.*, p. 26.
[556] Robert LEGROS, « Les notions à contenu variable en droit pénal », dans Ch. PERELMAN et R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 1984, 21, p. 21.
[557] Jean CARBONNIER, « Les notions à contenu variable dans le droit français de la famille », dans Ch. PERELMAN et R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 1984, 99, 99.
[558] *Id.*, 100.

Cet auteur propose de parler de notions « à contenu variable » et les oppose aux notions « à contenu fixe ». Pour lui, le contenu d'une notion n'est variable que dans la mesure de l'imprécision du contenant et il donne l'exemple du « secret professionnel », pouvant être un secret « absolu » ou « relatif », et nous fait remarquer que si le secret est « absolu », le juge n'a aucun problème de contenu à résoudre[559].

D. Bourcier souligne que normalement la plupart des études portant sur le standard commencent par énoncer que le standard est indéfinissable et que « seul un contenu peut lui être affecté »[560]. Toutefois, elle a voulu présenter une définition minimale dans le cadre de l'objet de sa recherche portant sur la police municipale et elle a suggéré une autre approche pour ce qui est du contenu du standard.

Ainsi, la définition minimale proposée met en jeu la fonction cognitive du standard, qui est à la fois normative et décisionnelle : « Un standard est un type de disposition faisant appel à un concept indéterminé d'origine législative, réglementaire et/ou jurisprudentielle dont la fonction consiste à relier certains faits à des règles en vue d'obtenir un effet déterminé, suivant des schémas de raisonnement pouvant donner lieu à la création d'autres standards ou d'autres règles »[561].

La doctrine souligne également la distinction devant être faite entre les notions à contenu variable d'origine légale ou lacunes *intra legem* et celles d'origine jurisprudentielle. La lacune *intra legem* est voulue et consciente et démontre que le législateur a voulu déléguer au juge la mission de la compléter[562].

Pour C. Castets-Renard, il faut déterminer également parmi les notions à contenu variable celles qui peuvent être qualifiées de notions-cadres et celles qui sont des standards juridiques. Ainsi, afin de bien cerner ce concept, elle signale que les notions-cadres ne sont pas totalement vagues et indéterminées, parce qu'elles vont évoluer au sein d'un cadre qui va délimiter leur interprétation, ce qui devient un

[559] R. LEGROS, préc., note 556, p. 29
[560] Danièle BOURCIER, *La décision artificielle : le droit, la machine et l'humain*, Paris, P.U.F., 1995, p. 57.
[561] *Id.*
[562] C. CASTETS-RENARD, préc., note 539, p. 29.

élément essentiel de leur définition. Le juge est donc celui qui va mettre en œuvre cette notion dans la pratique et, même si elles sont « vagues », elles sont toujours consacrées volontairement et le « flou conceptuel » qui les caractérise « est loin de signifier le retrait total du législateur et le silence législatif concerne uniquement la détermination du contenu normatif de la norme »[563].

De plus, ces notions-cadres sont des « notions fonctionnelles »[564] qui ont pour objet l'adaptation du droit et, selon cette auteure, sont destinées à appliquer la volonté politique du législateur, grâce à la mise en œuvre d'un droit qui se caractérise par la souplesse et la flexibilité.

À la « notion fonctionnelle » on peut opposer la « notion conceptuelle » qui est peu évolutive et à laquelle il est possible d'accorder une unique définition. Bien sûr, ces deux notions poussent à l'auteure à faire un parallélisme avec les notions cadres et les règles juridiques.

Pour certains, les standards juridiques vont présenter les mêmes caractères que les notions cadres, mais seuls les standards textuels sont des notions cadres, à cause de leur nature de « lacune interne à la loi »[565], pouvant affirmer également que la « normalité » est le caractère essentiel des standards textuels.

La doctrine n'hésite pas à reprendre certains exemples que le père de la jurisprudence sociologique, R. Pound, avait déjà qualifié de standards, tels que le « raisonnable », le « valable » ou le « loyal »[566].

---

[563] *Id.*, p. 85.

[564] *Id*,, p. 88.
Castets-Renard souligne également que le contenu de la notion fonctionnelle n'est jamais fixe ni connu *a priori*, puisqu'il va évoluer selon la situation, d'espèce, ce qui rend difficile le fait d'avoir une définition unique et prouve son contenu circonstanciel et ouvert, pouvant appréhender toute situation juridique nouvelle.

[565] *Id.*, p. 91.
Les exemples présentés sont la « bonne foi », « l'intérêt de la famille », « l'ordre public », le « bon père de famille », entre autres.

[566] Voir à ce sujet : Stéphane CAPORAL, « Édouard Lambert, Théoricien de la Jurisprudence Sociologique », *Acta Universitatis Danubius Juridica*, No.1/2009, 20, en ligne : http://www.juridica-danubius.ro/continut/arhiva/A117.pdf (consulté le 20 juin 2010).
Cet auteur souligne qu'Edouard Lambert définit le standard comme étant un « modèle et toise de conduite » et énumère un certain nombre, dont ceux que nous avons cité.
Voir également : C. CASTETS-RENARD, préc., note 539, p. 94.

Quand nous observons les dispositions relatives au principe de finalité, nous identifions très clairement que des termes de cette nature se trouvent présents dans la formulation des dispositions faisant référence à un tel principe, ce qui nous montre que le législateur a fait appel à cette technique dans ce contexte.
Afin d'utiliser une seule expression dans le cadre de notre recherche, nous avons considéré celle du standard comme étant celle qui convient à notre sujet. Même si cette notion reste assez polémique, elle est encore assez ouverte et, par conséquent, capable de représenter l'idée en toile de fond de la plupart des notions que nous analyserons. De plus, elle est l'expression qui s'adapte le mieux à notre recherche portant sur le droit européen et canadien, puisque même si elle tire son origine de la Common Law, elle est complètement intégrée aux théories propres au droit civil.

**2- Des notions à contenu variable, standards et principe de finalité**

Nous observons que c'est notamment dans l'hypothèse d'une réutilisation de l'information personnelle que la notion de « finalité » et le principe y faisant référence dévoilent les traits pouvant donner lieu à son assimilation avec un standard.
Et cela, parce que quand nous regardons les dispositions encadrant l'utilisation des renseignements personnels, il est facile pour nous d'identifier les caractéristiques d'une telle technique juridique.

Nous pouvons déjà affirmer que les éléments constituant ce principe de finalité dans les lois en la matière et dans ce contexte d'utilisation de l'information personnelle nous laissent deviner l'existence de traits caractéristiques d'un standard.

En observant la disposition qui encadre la « réutilisation » de l'information à caractère personnel que la Loi I et L modifiée propose dans le contexte français, nous identifions l'obligation visant à ce que les données personnelles de tout

traitement soient collectées pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités.

La Convention 108, les Lignes directrices de l'OCDE relatives à la protection de la vie privée et la Directive 95/46/CE font appel au critère de la « compatibilité » afin d'encadrer les utilisations ultérieures des données personnelles.

Le législateur français et européen a adopté plutôt le critère de la « compatibilité » entre les finalités d'utilisation de l'information dans les dispositions voulant limiter la réutilisation des données personnelles.
La notion de « finalités compatibles » a été utilisée par les interprètes des textes en la matière. Cette notion de finalité compatible ne se trouve pas explicitement dans la loi, mais elle sous-tend toutes les dispositions liant l'utilisation ultérieure des données à la condition de la compatibilité entre les finalités.

Le législateur canadien a prévu également pour le secteur public fédéral une disposition équivalente, en exigeant que, à défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne puissent servir à celle-ci qu'aux fins pour lesquelles ils ont été recueillis ou préparés par l'institution, de même que pour les usages qui sont compatibles avec ces fins.

Nous observons alors que le critère de la compatibilité a été choisi dans le cas canadien, au moins pour ce qui est du secteur public, et que le critère utilisé n'est pas celui de « l'acceptable », comme dans le cas du droit fédéral canadien relatif au secteur privé où le législateur a établi ce critère à appliquer à l'aide du test de la « personne raisonnable ».

En effet, pour le secteur privé canadien, la LPRPDE établit que l'organisation ne peut recueillir, utiliser ou communiquer les renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptable dans les circonstances.

Comme nous l'avons étudié dans les lignes précédentes, l'utilisation de ces critères a donné lieu à l'utilisation de la notion des « fins acceptables », que nous retrouvons très souvent dans les décisions des interprètes de la loi et dans la doctrine en la matière. Il y a eu un passage du critère de « compatible » vers « l'acceptable » et nous observons l'accompagnement de ce critère par celui de la personne « raisonnable », donnant lieu à une combinaison faisant appel à deux standards dans la formulation de la loi : « l'acceptable » et le « raisonnable ».

M. Moran a étudié le standard de la « personne raisonnable » et met en exergue une problématique que la doctrine analyse depuis des années : « ...*insight later voiced by feminists critical race theorists, and others, that there is something troubling about using an idealized person as a legal standard* »[567]. Cet auteur signale encore que « *it seems at least conceivable that adopting some ideal person as a standard of behaviour creates an almost irresistible opening to endow that imaginary person with all sorts of qualities that are not in fact prudential* »[568].

En effet, ce standard présente un certain danger quant à la possible création d'un « idéal » de personne qui ne correspondrait pas nécessairement à la réalité et qui, pourtant, serait à l'origine du standard « objectif », avec tous les problèmes que cela peut poser.

Toutefois, ce standard reste encore un instrument d'une grande utilité et, comme certains l'ont souligné, le recours aux standards légaux de la LPRPDE est devenu un outil d'une grande importance : « *Legal Standards such as "reasonableness" are used extrensively in the Act because it must be applied in a wide range of situations, but such standards are defined : principles and specially related guidelines set out their general rationale and scope* »[569].

---

[567] Mayo MORAN , *Rethinking the Reasonable Person: An Egalitarian Reconstruction of the Objective Standard*, New York, Oxford University Press, 2003, p. 1.
[568] *Id.*, p. 16.
[569] P. TRUDEL et F. ABRAN, préc., note 499, p. 30.

En tout cas, l'exemple de la « personne raisonnable » dans le texte canadien confirme une tendance qui est celle d'avoir recours à ce type de technique législative en cette matière.

Nous observons alors « un type de disposition faisant appel à un concept indéterminé d'origine législative »[570], pouvant nous faire penser à un standard. Et nous constatons que, dans le contexte de la protection des renseignements personnels, l'utilisation des notions de cette nature est constante. Elles sont très faciles à identifier quand il s'agit d'encadrer des questions telles que la finalité des renseignements personnels ainsi que leur qualité, ce qui motive sans doute que l'on puisse trouver que des articles imposant que tels renseignements soient « adéquats », « pertinents », « non excessifs » par rapport à la finalité.

Dans d'autres dispositions, nous retrouvons l'obligation visant à assurer que les finalités sont « explicites », « légitimes » et « déterminées ». Parfois la condition vise à établir que les traitements ont été effectués « licitement » et « loyalement ». Dans tous les cas, des critères tels que « l'adéquat », le « pertinent », le « licite » et le « loyal », entre autres, nous laissent deviner que le législateur a fait encore appel à cette technique.

Nous reconnaissons ici l'utilisation de standards juridiques que certains qualifient de « textuels » et qui, selon la doctrine, sont des « notions cadres d'un genre particulier, enserrés dans des directives de normalité, au sens de moyenne et modèle »[571]. Cette définition du standard comme « *modèle* à respecter et de *moyenne* de comportement des individus constituant une société »[572] paraît rejoindre celle de la majorité de la doctrine et nous permet d'identifier ces standards juridiques textuels dans la formulation des dispositions présentes dans les lois en matière de protection des renseignements personnels.

---

[570] D. BOURCIER, préc., note 560, p. 57.
Cette expression est utilisée para Danièle Bourcier dans la définition minimale du standard qu'elle propose.
[571] C. CASTETS-RENARD, préc., note 539, p. 98.
[572] *Id.*, p. 95.

Pour certains, seul le standard renvoie à la « normalité », ce qui ne caractérise pas la totalité des notions à contenu variable, puisque le standard vise « ce qui est et doit être », au sens de « moyenne » et de « modèle »[573].

De plus, le standard juridique comprend non seulement la normalité juridique, mais également la « normalité sociale », et cela parce qu'il prend en compte la moyenne sociale[574]. Le « raisonnable », « l'acceptable » ou le « compatible » s'approchent de cette idée de façon très claire et évidente.
Pensons encore au « raisonnable » et à « l'acceptable » qui peuvent également évoluer et changer dans le temps et l'espace et peuvent répondre à l'idée d'un contenant qui ne change pas et à un contenu qui change constamment.

Pour ce qui est de cette question dans le contexte du principe de finalité, nous pouvons reconnaître cette caractéristique dans des notions telles que les « finalités compatibles » ou les « usages acceptables », toutes deux résultant de la lecture des dispositions européennes et canadiennes en la matière comme du travail de l'interprète et de la doctrine.

Toutes deux se caractérisent par un contenant qui reste fixe et un signifiant qui peut varier dans le temps et dans l'espace.
De plus, ce type de standard rentre dans la catégorie des « standards formels » qui, selon certains, se caractérisent par la présence dans leur expression d'un qualificatif ou d'un adverbe[575]. En effet, pour S. Rials, l'adjectif qualificatif et l'adverbe semblent les formes grammaticales essentielles du standard[576].

---

[573] Voir à ce sujet : C. CASTETS-RENARD, préc., note 539.
[574] *Id.*, p. 100.
[575] D. BOURCIER, préc., note 560, p. 57.
Danièle Bourcier fournit l'exemple des « mesures insuffisantes » pour illustrer cette catégorisation.
[576] Stéphane RIALS, *Le juge administratif français et la technique du standard (essai sur le traitement juridictionnel de l'idée de normalité)*, Paris, L.G.D.J., 1980, p. 45.

Ces expressions se rapprochent également de la définition caractérisant les « notions à contenu variable », d'après ce que nous avons pu voir dans les lignes précédentes.

Et cela parce qu'en réalité des finalités qui peuvent être considérées comme compatibles à un moment précis, peuvent ne plus l'être plus tard, à cause de changements majeurs dans l'appréciation concrète ou de l'apparition de nouveaux risques dérivés du rapprochement de certaines informations qui étaient plutôt neutres dans le passé.

**3- Dialogue entre standards et vie privée**

La notion de « personne raisonnable » peut nous faire penser *a priori* qu'il s'agit d'un standard et elle a été utilisée par le législateur canadien de façon à aider dans la détermination des finalités acceptables d'utilisation des renseignements personnels. Ainsi, nous observons dans la loi canadienne pour le secteur privé que certaines expressions s'utilisent dans la disposition encadrant les « fins acceptables ». Et cela parce que le législateur établit un test de la « personne raisonnable » qui estimerait « acceptables dans les circonstances » les fins auxquelles l'organisation recueille, utilise et communique des renseignements personnels.

Nous identifions ici très clairement comment certains standards « s'inscrivent dans une structure dynamique où sont confrontés, lors de la prise de décision, d'autres standards largement dépendants, dont seuls certains peuvent être quantifiés »[577].

En effet, nous observons par la rédaction de cette disposition de la LPRPDE que chaque standard utilisé par le législateur va dépendre d'un autre. Les renvois d'un standard à l'autre se font en effet continuellement, donnant lieu à une dynamique très particulière.

[577] D. BOURCIER, préc., note 560, p. 63.
Bourcier présente l'exemple de la « tranquillité publique » pour montrer qu'un standard est éminemment dialectique et qu'il doit nécessairement être considéré dans le cadre d'une structure dynamique.

D'autres auteurs nous parlent d'une « étroite imbrication » de certaines notions, qui va les faire dépendre les unes des autres[578], chose qui, selon nous, se produit dans certaines dispositions encadrant les « finalités acceptables » dans la réutilisation de l'information.

Regardons par exemple l'analyse qui doit se réaliser en plusieurs temps à cause de l'établissement de trois paramètres visant à déterminer ce qui justifie la communication ou l'utilisation des renseignements personnels, à partir de la LPRPDE canadienne[579]. La nature de ces paramètres, nous fait penser à des standards devant être interreliés.

Le critère de l'acceptable (paramètre un) et celui du raisonnable (paramètre deux), doivent tous les deux être appréciés dans les circonstances (paramètre trois), ce qui met en relief un jeu de « renvois » qui démontre le degré de complexité auquel fait face l'interprète de la loi.

Nous assistons alors à un processus de dialogue entre les différents standards, pouvant même nous faire penser à un « réseau neuronal » formé par ces standards interconnectés. Ce dialogue se déclenche, facilite et structure le raisonnement à l'aide d'autres standards.

Nous constatons que le critère du « raisonnable » est d'une grande importance à l'heure de déterminer si les fins sont « acceptables dans les circonstances » ou pas, ce qui nous oblige à observer que l'autorité de contrôle et le juge jouent un rôle majeur au moment d'établir ce qui est raisonnable ou ce qui ne l'est pas. La subjectivité dans cette analyse n'est pas un facteur à négliger pour ce qui est de l'établissement des conditions de l'utilisation et la communication des renseignements personnels. Toutefois, pour certains, « les définitions données par

[578] C. CASTETS-RENARD, préc., note 539, p. 114.
Pour Castets-Renard, nous observons dans le cadre du droit d'auteur, une étroite imbrication des notions « d'auteur », « d'œuvre » et de « création » qui les fait dépendre les unes des autres.

[579] Le paragraphe 5(3) de la LPRPDE dispose que « l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances »

le procédé des renvois mutuels paraissent succinctes et incomplètes mais suffisent sur le principe à constituer des directives d'interprétation »[580].

La loi belge relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[581] a renforcé le principe de finalité suite à sa modification en 1998, avec une disposition faisant appel à des notions pouvant nous faire penser aux standards et qui ne se trouvent pas dans la Directive 95/46/CE.

Ainsi, à l'article 4.2, cette loi établit que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé.

Cette loi introduit alors les paramètres des « facteurs pertinents » et de « prévisions raisonnables de l'intéressé » dans le dialogue entre standards devant aider à déterminer quelles sont les « finalités compatibles ».

L'autorité belge utilise notamment le critère de « prévisions raisonnables de l'intéressé » comme paramètre pour décider de l'utilisation des renseignements personnels. Par exemple, si un organisme public désire partager les données contenues dans les traitements qu'il détient et qu'elle considère que le citoyen va pouvoir prévoir un tel transfert des données le concernant, elle va produire un avis positif.

En tout cas, nous constatons un renvoi vers le critère des « prévisions raisonnables de l'intéressé », qui nous fait penser à celui qui se réalise en droit canadien pour ce qui est du secteur privé, faisant appel à la personne raisonnable.
Le législateur belge a encore laissé une marge plus vaste et flexible à l'interprète, en incluant dans cette disposition « tous les facteurs pertinents » pouvant aider à

[580] C. CASTETS-RENARD, préc., note 539, p. 115.
[581] Nous avons déjà fait mention à ce texte dans les pages précédentes afin d'analyser comment le principe de finalité a été adopté par le législateur belge .

déterminer si les finalités d'utilisation des renseignements personnels sont compatibles.
Toutefois, le critère du « raisonnable » est toujours le standard privilégié à utiliser dans l'évaluation au cas par cas que les autorités de contrôle réalisent. Cela nous montre que les renvois d'un standard à l'autre, qui tirent parfois leur origine du travail du législateur, est devenue la pratique actuelle des autorités de contrôle des deux côtés de l'Atlantique.

Comme certains l'ont souligné, quand on parle de la réutilisation des données disponibles au sein d'une administration, nous sommes face à une opération complexe et dangereuse. Certains auteurs observent divers critères utilisés à l'heure d'apprécier concrètement le respect des « prévisions raisonnables de l'intéressé », « sans que l'on comprenne la logique des choix posés par la Commission (belge) »[582], pouvant déjà paraître subjectifs et peu argumentés.

Le besoin de définition des critères d'actuation à l'heure d'utiliser certains standards semble également être le défi majeur. Nous observons ces difficultés en Europe et au Canada, où il nous semble difficile d'identifier quels sont les critères et la méthodologie utilisés afin de comprendre si en effet la démarche des autorités suit de façon générale un schéma particulier.

De plus, nous notons que le degré d'acceptabilité des fins est un concept pouvant nous paraître assez flou et indéterminé, qui doit être évalué grâce à des concepts tels que la « proportionnalité » et la « légitimité », ce qui pousse à un renvoi perpétuel d'une notion vers les autres. Ce test de la « personne raisonnable » nous oblige également à devoir en tout temps évaluer au cas par cas, et cela parce que ce qui est « acceptable » doit être guidé par le critère d'une personne raisonnable, mais toujours « dans les circonstances », ce qui oblige à réaliser une analyse pour chaque cas qui se présente.

[582] Élise DEGRAVE, « Principe de finalité et secteur public dans la jurisprudence de la Commission de la protection de la vie privée », *Chroniques de droit public*, issue 1, 2009, 46, 70.

Pour D. Bourcier, le contenu de certains standards, qu'elle étudie dans le cadre de sa recherche sur la police municipale et qui sont parfois imbriqués, n'a pas d'intérêt puisqu'il intervient dans un « réseau d'implications et d'inférences que seules les corrélations peuvent éclairer»[583].

**4- L'éclatement des standards en « sous-standards »**

Il faut remarquer l'idée exprimée par le Professeur Ghestin selon laquelle, « c'est l'ensemble des applications faites par le législateur en utilisant la notion à contenu variable ou des solutions données par le juge qui permet, graduellement, d'élaborer une définition, ou tout au moins de délimiter positivement et négativement la notion, autrement dit de savoir ce qui rentre ou non sous cette qualification »[584].

Pensons par exemple aux notions de « fins acceptables », « usage compatible » ou tout simplement au « compatible » et nous pouvons imaginer les difficultés pour la délimitation et même la définition de tels concepts.

Le CPVPC soulignait en 1995 la difficulté d'expliquer ce qu'on entend par un « usage compatible » et affirmait qu'il est plus facile de définir le contraire, soit un usage incompatible[585]. En effet, ce type de standard se délimite plutôt négativement puisqu'il est plus facile de le définir ainsi que de le faire positivement.

Il sera alors plus facile dans un premier temps d'identifier quelles sont les finalités incompatibles et, par contre, il peut vraiment devenir problématique de définir celles qui seront jugées compatibles au cas par cas.

Ce que nous avons observé en analysant ce principe de finalité est qu'un « éclatement » du standard se produit, et cela par l'apparition d'autres sous-standards de nature plutôt jurisprudentielle.

---

[583] D. BOURCIER, préc., note 560, p. 80.
Dans ce texte on fait référence concrètement aux « standards circonstanciels ».

[584] Jacques GHESTIN, « L'ordre public, notion à contenu variable, en droit privé français», dans Ch. PERELMAN et R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 1984, 77, p. 78 (nous soulignons).

[585] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 337, p. 82.

Ces notions, nous les retrouvons dans les décisions ou délibérations émanant des autorités de contrôle, ainsi que dans les rapports et textes qu'ils produisent. Pensons aux notions de « finalités acceptables » ou « usages compatibles » dont on a largement parlé dans les pages précédentes.
Nous observons également que même si ce sont des notions utilisées très souvent, elles n'ont pas fait l'objet d'un grand développement de la part de la doctrine.
Nous retrouvons encore le produit de cet éclatement notamment dans des notions telles que « finalité principale », « finalité secondaire », « double finalité », « finalités multiples », « finalités complémentaires », « dualité de finalités », « utilisation compatible », « finalité initiale », « fichiers à finalité distincte » ou « traitement à finalité unique ».
« Fins conformes » et « fins premières » sont de même des expressions qui nous montrent que ces standards, qui ne trouvent pas leur origine dans les lois, proviennent du travail réalisé par l'interprète de la loi ou par la doctrine.

Nous constatons alors l'existence d'un ensemble de standards de différente nature, reliés au principe de finalité. D'origine législative, jurisprudentielle ou doctrinale, ils démontrent la complexité d'une telle notion et de son développement.

Finalement, nous devons noter que cette technique du standard appartient plutôt au droit anglo-saxon or c'est précisément dans le contexte du droit américain que l'application des standards était confiée à des commissions administratives plutôt qu'à des tribunaux judiciaires[586].
La raison qui a motivé cette tendance américaine est que ces commissions administratives étaient plus indiquées pour juger des questions pour lesquelles il était nécessaire de pouvoir compter sur de vastes connaissances techniques et sur l'avis de vrais « experts » en la matière.

Dans le domaine de la protection des renseignements personnels en Europe et au Canada, les autorités de contrôle sont en charge du respect des lois en la matière.

[586] M. O. STATI, préc., note 535, p. 101.

Ces autorités de nature plutôt administrative et indépendantes sont celles qui doivent se manifester sur les questions relatives à la protection des renseignements personnels. Ce qui nous indique encore que le domaine de la protection des renseignements personnels rejoint en grande partie toutes les caractéristiques définissant cette technique du standard et son interprétation.

## SECTION 2 La démarche dans la détermination des contours du principe de finalité dans la pratique

Les autorités de contrôle sont les plus importants interprètes du principe de finalité. Dans le cadre de notre étude, nous avons analysé l'interprétation qui a été faite au Canada par l'autorité de contrôle dans la matière, le CPVPC, et nous avons étudié la doctrine de la CNIL, autorité de contrôle en France et interprète du principe de finalité depuis des années.

Il s'agit maintenant de comprendre comment les autorités de contrôle opèrent face à la présentation d'une plainte de la part de citoyens suite au non-respect des législations en la matière, et cela afin de comprendre comment se présente le conflit à analyser ou comment ces autorités parviennent à établir les équilibres nécessaires pour le respect du principe de finalité relatif au traitement des données personnelles. L'analyse des « données brutes », que les autorités examinent avant d'adopter des décisions, nous aidera à identifier les éléments les plus intéressants d'une telle démarche.

Dans un deuxième temps, nous analyserons les mécanismes plus ou moins théoriques dont les autorités de contrôle et les juges disposent afin de régler les conflits entre droits ou entre le droit à la vie privée et d'autres intérêts, tel que l'intérêt général.

### 1- Les autorités de contrôle et les faits : étude des dossiers

Nous avons pu connaître une partie de la doctrine que la CNIL produit depuis des années pour ce qui relève de la définition et de la délimitation des contours du principe de finalité consacré par la législation française.

Nous avons pu comprendre également comment le CPVPC établit des lignes directrices pour arriver à cerner les limites du critère des « fins acceptables» en droit canadien.

L'exercice que nous voulons entreprendre dans cette partie de notre étude vise à saisir quel est le travail auquel se livrent les « décideurs » et arbitres, face au conflit

existant entre le droit à la protection des données personnelles et un autre droit ou intérêt.

Si nous cherchons à examiner le mécanisme d'analyse qui se déclenche dans cette recherche d'équilibre, c'est pour essayer d'identifier les outils qui sont à la portée de l'autorité de contrôle ou du juge.
Dans une première partie, nous analyserons un petit échantillon des « données brutes » formant chaque dossier suite à la présentation d'une plainte qui place le principe de finalité au centre du débat. Nous procéderons à l'analyse de ces données grâce à une grille d'analyse capable de faire ressortir les éléments intéressants dans le cadre de notre recherche.

Ainsi, nous avons jugé nécessaire de procéder également à l'étude des cas correspondant à des dossiers comportant des plaintes de citoyens, les rapports d'enquête, toutes les autres communications et tous les documents pertinents dans le cadre de l'analyse d'une telle plainte.
Et cela, dans le but de retenir fondamentalement une vision plutôt « factuelle » et de comprendre quels sont les « faits » autour du sujet qui nous occupe.
Nous avons voulu comprendre à quelle occasion le respect du principe de finalité a été invoqué par les citoyens et comment il doit servir à déterminer si le traitement, l'utilisation ou la communication de renseignements personnels a été réalisé en respectant l'esprit de ce principe.

Nous avons constaté que, dans le contexte du droit à la protection des données personnelles, les autorités de contrôle ont un rôle majeur dans l'interprétation des règles et principes contenus dans les lois en la matière.
Elles sont également compétentes pour trancher un conflit entre deux libertés, parfois antagonistes, ou entre une liberté individuelle et l'intérêt général, afin de pondérer les intérêts en présence.

Cette tâche a été traditionnellement accordée au juge constitutionnel, qui avait un grand pouvoir d'appréciation qui, selon certains auteurs, s'explique par la fonction proprement politique qu'il exerce[587]. Aujourd'hui, ce grand pouvoir d'appréciation appartient non seulement au juge constitutionnel, mais également aux autorités de contrôle de protection du droit à la vie privée.
Il nous faut donc commencer par comprendre quelle est la nature des deux autorités de contrôle des deux côtés de l'océan Atlantique qui font l'objet de notre étude.

### 2- Le Canada et l'Europe : les autorités de contrôle et les questions relatives au principe de finalité

Il s'agit maintenant d'étudier quelle est la nature des autorités de contrôle en charge de surveiller l'application des lois en matière de protection des renseignements personnels. Ainsi, le CPVPC, en vertu de son mandat, a la responsabilité de surveiller le respect de la LPRP, qui encadre le traitement des renseignements personnels, utilisée par les ministères et organismes fédéraux ainsi que de la LPRPDE, applicable au secteur privé. Le CPVP a pour mission de protéger et de promouvoir le droit des personnes à la vie privée des Canadiens.

Le CPVPC reçoit et fait enquête sur les plaintes déposées par les personnes qui prétendent que des renseignements personnels les concernant et détenus par une institution fédérale ont été utilisés ou communiqués sans leur consentement, lorsque cela arrive dans des cas non prévus par les articles 7 ou 8 de la LPRP.

Pour ce qui relève des questions ayant trait aux renseignements personnels dans le secteur privé, le CPVPC peut examiner toutes les plaintes déposées en vertu de la LPRPDE, sauf dans les provinces qui ont adopté des lois essentiellement similaires à la loi fédérale en matière de protection des renseignements personnels[588].

---

[587] François RIGAUX, « Le contrôle de la légitimité constitutionnelle ou internationale de la loi et des décisions judiciaires », dans François RIGAUX (dir.), *La vie privée, une liberté parmi les autres?*, Travaux de la Faculté de droit de Namur, t. 17, Bruxelles, Larcier, 1992, 23, p. 47.
[588] Il faut noter que le Québec, la Colombie-Britannique et l'Alberta ont déjà adopté des lois en la matière. Nous observons une situation équivalente pour ce qui est de l'Ontario, en ce qui concerne

Il faut noter que, même dans les provinces qui ont adopté une loi essentiellement similaire, et partout ailleurs au Canada, la LPRPDE s'applique toujours à tous les renseignements personnels recueillis, utilisés ou communiqués par toutes les entreprises fédérales, y compris les renseignements personnels au sujet des employés de celles-ci.

Cette loi s'applique également à toutes les données personnelles qui circulent d'une province ou d'un pays à l'autre, dans le cadre d'activités commerciales impliquant des organisations assujetties à cette loi ou à une loi essentiellement similaire.

L'autorité canadienne travaille de façon autonome et n'a aucun compte à rendre à d'autres entités du gouvernement pour examiner les plaintes provenant de personnes concernant le secteur public fédéral ou le secteur privé. Étant donné que le commissaire relève directement de la Chambre des communes et du Sénat, et non du gouvernement en place, l'indépendance et l'impartialité sont assurées.

Nous pouvons affirmer que le CPVPC agit plutôt comme un ombudsman pour les plaintes concernant la vie privée. Le Commissaire va pouvoir enquêter sur les plaintes, les examiner, publier des rapports annuels et des recommandations, effectuer des vérifications, créer une prise de conscience chez les citoyens et entreprendre des recherches en la matière.

La CPVPC tient à régler les plaintes par le biais de la négociation, en se servant des techniques de médiation et de conciliation s'il y a lieu.
Cependant, si les parties ne collaborent pas, le CPVPC peut convoquer des témoins, faire prêter serment et exiger la production d'éléments de preuve. Il faut noter que, dans certains cas qui demeurent toujours irrésolus, plus particulièrement en vertu de la LPRPDE, le commissaire peut saisir la Cour fédérale de l'affaire et demander à cette dernière d'émettre une ordonnance pour rectifier la situation.

---

les renseignements personnels sur la santé, en vertu de la loi ontarienne sur la protection des renseignements personnels sur la santé.

L'autorité de contrôle française, la CNIL, a été instituée par la Loi I et L et possède une nature d'autorité administrative indépendante. Cette autorité de contrôle tire son caractère d'indépendance de son organisation et de sa composition. Ses décisions sont adoptées en séance plénière et peuvent faire l'objet d'un recours devant la juridiction administrative.

La CNIL émet des avis sur des projets de loi suite à la demande du Gouvernement et produit des rapports en matière du droit à la protection des données personnelles. Elle est investie d'une mission générale d'information des personnes, elle régule et recense les fichiers, c'est-à-dire la liste des traitements qui lui ont été déclarés. La Loi I et L modifiée a doté la CNIL de nouveaux pouvoirs de contrôle et de sanction. Ainsi, les missions de contrôle de la CNIL s'inscrivent dans un calendrier annuel de contrôle ou existent en réponse à certains besoins, tels que le dépôt d'une plainte ou suite à une demande à tel effet.

Pour ce qui est du pouvoir de sanction de la CNIL, nous observons que cette autorité dispose de certaines mesures coercitives ainsi que de la possibilité d'imposer des sanctions pécuniaires. Il faut noter qu'une exception existe quant à la capacité d'imposer des sanctions pécuniaires pour ce qui est des traitements mis en œuvre par l'État.

Nous identifions des différences majeures en ce qui concerne la nature même du CPVPC, qui est plutôt un « ombudsman » et qui a la capacité de saisir la Cour fédérale afin de protéger le droit à la vie privée des Canadiens, et la CNIL qui s'est vu accorder la capacité de sanctionner directement le non-respect des dispositions de la Loi I et L modifiée.

Nous observons également que, pour les années 2008-2009 pour ce qui est du CPVPC et dans le contexte du secteur public, les cas relatifs à la collecte, l'utilisation, la communication, la conservation ou le retrait des renseignements

personnels supposent un total de 220 plaintes sur les 990 qui ont donné lieu à une enquête, ce qui représente environ 23 %[589].

Il faut noter que, comme au cours des exercices précédents, les plaintes les plus fréquentes soumises au CPVPC concernent l'accès aux renseignements personnels et les délais de réponse, représentant pour les années 2008-2009 respectivement 38 % et 34 % de l'ensemble des plaintes.

Par contre, le nombre de plaintes relatives à l'utilisation et à la communication de renseignements personnels s'élève à 171 cas, soit 23 %. Pour ce qui est de la collecte, nous observons que seules 9 plaintes ont été présentées au CPVPC, ce qui représente seulement 3 % de la totalité des plaintes. Nous faisons ici référence aux cas où les renseignements personnels ont été utilisés ou communiqués sans le consentement de la personne concernée et ne satisfont pas à l'un des critères d'utilisation ou de communication permise sans consentement aux articles 7 et 8 de la LPRP.

Il faut noter également qu'en vertu de l'article 41 de la LPRP, la Cour fédérale canadienne ne peut se pencher que sur le refus d'un organisme fédéral de communiquer les renseignements personnels demandés en vertu de la LPRP. Ainsi, la Cour fédérale ne peut pas réviser les cas relatifs à la collecte, l'utilisation ou la communication injustifiée des renseignements personnels par une institution gouvernementale. Le CPVPC avance que c'est la raison pour laquelle peu de décisions de justice sont motivées en la matière : « D'ici là, en raison de la grande limitation des motifs de recours des tribunaux en vertu de la LPRP au cours des années demeure très faible »[590].

[589] Voir sur ces pourcentages le dernier rapport annuel concernant la LPRP : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2008-2009 concernant la Loi sur la protection des renseignements personnels*, 2009.
[590] *Id.*

Pour ce qui est des plaintes reçues par le CPVPC en vertu de la LPRPDE et dans le cadre de la gestion des renseignements personnels dans le secteur privé, nous observons que, pour l'année 2008, 162 étaient relatives à l'utilisation et à la communication et 93 à la collecte. Ainsi, 38 % portaient sur la manière dont les organisations ont utilisé et communiqué les renseignements et le type le plus courant allègue que les renseignements personnels auraient été utilisés à des fins autres que celles pour lesquelles ils avaient été recueillis et auraient été communiqués à des tiers sans le consentement de la personne concernée. Les plaintes qui portent sur la collecte font normalement référence au cas de collecte des renseignements personnels sans le consentement approprié ou sur la collecte de plus de renseignements qu'il n'est nécessaire pour remplir le but visé par la collecte[591]. Il faut noter également que la plupart des plaintes en vertu de la LPRPDE touchent au secteur financier.

En 2008, la CNIL a reçu 4 244 plaintes pour non-respect de la Loi I et L, portant notamment sur commerce (25 %), banque-crédit (25 %), travail (15 %), opérateurs télécoms (10 %) et d'autres thèmes divers (10 %)[592]. Nous observons donc un nombre presque inexistant de plaintes tirant leur origine de la collection, l'utilisation ou la communication de renseignements personnels dans le cadre du secteur public.

Même si cela varie d'une année à l'autre, nous observons uniquement une dizaine de plaintes concernant le secteur public présentées à la CNIL par an. Cela prouve que le fait reste assez marginal ou qu'il est rare de recevoir ce type de plaintes et que la majorité vise plutôt la dénonciation de la gestion des données personnelles par le secteur privé. Dans la plupart des cas, quand elles visent le secteur public il

[591] Voir sur tous ces chiffres faisant référence aux plaintes en vertu de la LPRPDE : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2008 sur la Loi sur la protection des renseignements personnels et les documents électroniques*, 2009.

[592] Voir : COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *29 Rapport d'activité*, Paris, La Documentation française, Paris, 2009.

s'agit de dossiers liés aux traitements relatifs à la sécurité sociale et aux caisses d'assurance maladie.

Le nombre de plaintes pour les années 2008 et 2009 présentées aux autorités canadienne et française de contrôle représente la moyenne que nous observons dans les dernières années.

Nous constatons que les plaintes relatives au secteur privé sont, en général, plus nombreuses que celles relatives au secteur public. Celles qui font référence à l'utilisation et à la communication de renseignements personnels par les organismes publics sont spécialement rares dans le cas français. Au Canada, nous constatons que chaque année certaines plaintes dénoncent la mauvaise gestion des informations personnelles par les organismes du secteur public canadien.

Nous pouvons avancer déjà certaines hypothèses sur l'origine des différences entre le pourcentage de plaintes présentées concernant le secteur public face aux deux autorités de contrôle. Il nous semble que si l'on regarde celles qui concernent la communication et l'utilisation de renseignements personnels par les organismes publics sans le consentement des personnes concernées, nous identifions probablement des pistes à creuser.

Si l'on observe le cas français, nous pouvons penser que les solides contrôles *a priori* peuvent motiver une telle absence de plaintes. Quand nous observons les cas où des interconnexions ont été mises en place, nous identifions de grandes formalités déclaratives de la part du responsable du traitement et un mécanisme très lourd de validation qui se déclenche auprès de la CNIL.

Si nous observons le cadre *ad hoc* qui a été établi afin de contrôler la légitimité d'une telle interconnexion entre fichiers publics à cause des risques potentiels qui entourent une telle opération, nous constatons que l'accent est mis sur l'examen *a*

*priori* et cela fait que, pour le citoyen, le système qui en résulte est fiable et respectueux de ses droits.

Il est assez surprenant de voir le nombre réduit et même inexistant de plaintes faisant référence au non-respect du principe de finalité et, en conséquence, au non-respect de la finalité initialement déclarée d'un fichier géré par une institution publique. Nous trouvons pourtant une abondante doctrine dans les délibérations et avis visant à établir les conditions de la mise en place d'une interconnexion de fichiers et sur la nécessité de respecter les finalités initiales des fichiers en question. Dans le cas canadien, le fait que les dispositions dans la LPRP font une énumération stricte des cas où les organismes fédéraux peuvent échanger leurs renseignements personnels sans leur consentement fait que les citoyens dénoncent le non-respect de ces dispositions.

Nous observons alors que le CPVPC réalise plutôt un examen *a posteriori* de la validité de certains échanges ou connexions entre les fichiers publics, suite à la présentation d'une plainte d'un citoyen. Dans la majorité des cas, le CPVPC sait, grâce aux plaintes déposées par les citoyens, si un traitement respecte ou non les dispositions de la LPRP. La CNIL connaît normalement la conformité des traitements au moment de la déclaration du fichier.

Cela ne veut pas dire que le CPVPC ne réalise en aucun cas des contrôles avant la mise en place des rapprochements de données, puisque son avis est demandé avant la mise en place de projets visant à mettre en relation des fichiers du secteur public canadien.

Pour cette raison, la réalisation d'« évaluations sur les facteurs relatifs à la vie privée » est de plus en plus importante, évaluations qui demandent un contrôle *a priori* des traitements et de leurs interconnexions. Il faut tenir compte également de l'existence d'un répertoire *Info Source* grâce auquel on peut connaître quelles utilisations ont été faites des renseignements personnels contenus dans les

traitements du secteur public. Ce répertoire des « utilisations » autorisées des traitements détenus par les organismes publics aide également les citoyens à identifier les cas où ils considèrent que des communications et utilisations de leurs renseignements personnels ne sont pas justifiées.

Il faut noter que le CPVPC n'a pas le pouvoir de ne pas autoriser ces possibles utilisations des traitements du secteur public et qu'il ne peut qu'essayer de « négocier » la non autorisation de certains de ces usages.

**3- L'étude des « données brutes » : méthodologie**

Dans notre analyse des informations contenues dans les dossiers d'enquête du CPVPC et dans les dossiers relatifs aux plaintes adressées à la CNIL nous avons procédé avec une méthodologie, visant à faire ressortir les aspects pouvant nous éclairer dans le cadre de nos recherches.
Ce que nous avons voulu principalement examiner, c'est la manière dont la présence des standards peut influencer la prise de décision des autorités de contrôle. Il s'agit alors surtout de continuer à vérifier la présence de standards dans ce domaine, mais cette fois-ci en observant comment ils se présentent quand nous observons les « données brutes » qui motiveront plus tard une décision de l'autorité de contrôle.

De plus, nous avons voulu savoir quels sont les faits qui entourent l'application du principe de finalité dans le contexte du partage et du transfert d'information à caractère personnel entre les organismes du secteur public.

De la même façon, nous avons voulu comprendre comment s'applique ce principe dans le secteur privé quand des informations relatives à une personne sont transférées à un tiers. Nous avons privilégié une vision plutôt factuelle, afin de faire le lien entre les principes à respecter et les « faits ».

À l'aide d'une grille d'analyse, nous avons essayé de comprendre, d'une part, quels sont les cas de communication de renseignements personnels qui ont lieu au sein de l'administration et du secteur privé sans le consentement de la personne concernée, afin de voir comment les autorités de contrôle déterminent si le principe de finalité a été ou non respecté et comment ce principe s'interprète ; et d'autre part, nous avons cherché à savoir quels sont les intérêts se trouvant au centre de ces dossiers et pouvant représenter des valeurs à protéger, et cela, en détriment du droit à la protection de la vie privée. Il s'agit également de voir comment ces valeurs sont formulées, puisque nous tentons de vérifier quels sont les intérêts se trouvant face au principe de finalité dans les dossiers en question.
Il s'agit parfois de déterminer quelle a été la justification des ces transmissions d'information ou, plus concrètement, quel est l'élément qui est face au paramètre de la finalité. Il faut ici identifier quels sont les autres intérêts invoqués dans les dossiers de ce type lors de la présentation d'une plainte devant les autorités de contrôle.

Finalement, nous avons voulu identifier non seulement les « standards » se trouvant dans ces dossiers, mais également d'autres possibles « sous-standards », comme résultant de « l'éclatement » du principe de finalité que nous avons évoqué dans les pages précédentes.

L'objet de cet examen est fondamentalement de nous éclairer quant à la technique utilisée dans les dossiers de ce type et de voir comment l'application de ce principe se réalise dans la réalité.

La méthodologie choisie pour procéder à un tel examen se base sur l'utilisation d'un modèle de grille devant nous servir à identifier certains éléments dans chaque dossier examiné au sein des autorités de contrôle.
En droit canadien, nous avons été intéressés par l'analyse de la notion des « fins acceptables », raison pour laquelle nous avons analysé, au sein du CPVPC un ensemble de dossiers d'enquête choisis au hasard des cas où la LPRPDE a été

invoquée, afin d'examiner comment la question du partage d'informations personnelles sans le consentement des personnes concernées s'analyse dans la pratique.

Dans le cas du Canada, l'existence de deux lois différentes pour les secteurs public et privé marque la frontière entre les deux types de dossiers. Dans la LPRPDE, applicable dans le secteur privé, l'équivalent du principe de finalité devant être respecté pour tout traitement de données se trouve dans la section 5.3 qui porte sur les « fins acceptables », notion mise en rapport avec le « Test de la personne raisonnable »[593]. Il est très important pour nous d'analyser comment se réalise ce jeu de « renvois » entre standards sous ce texte de loi canadien.
Dans les dossiers d'enquête examinés au CPVPC, cette section ainsi que d'autres sections de la LPRPDE ont été invoquées, notamment celles portant sur la « Communication de renseignements personnels à l'insu de l'intéressé et sans son consentement »[594]. Tous les dossiers examinés avaient été fermés entre 2001 et 2006.

Pour ce qui est des dossiers examinés à la CNIL, nous avons retenu un groupe choisi au hasard parmi ceux qui dénonçaient à leur origine le non-respect de l'article 6.2º et 6.3º de la Loi I et L modifiée[595], qui encadrent le principe de finalité en droit français et qui font apparaître le critère des « fins compatibles »·.

Nous pouvons observer notamment des cas où des fichiers constitués pour une finalité concrète et dans le cadre d'une mission de service public ont été utilisés à d'autres fins, manquant de cette manière aux obligations que l'article 6.2º de la Loi I et L modifiée établit. Les dossiers examinés ont été traités à la CNIL après l'adoption de la Loi I et L modifiée.

[593] Il faut se rappeler que cet article dispose que « L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptable dans les circonstances ».
[594] Notamment la Section 7.3) de la LPRPDE.
[595] Il faut noter également que l'article 6.5º de la Loi I et L a été également invoqué dans les dossiers ayant fait l'objet de notre analyse.

Bien sûr, l'anonymat des personnes concernées a été fortement protégé durant tout le processus d'examen d'une telle documentation au CPVPC et à la CNIL.

La question qui motive un tel examen est également de savoir précisément comment les autorités de contrôle arrivent à identifier quelles sont les « finalités compatibles » avec la finalité première, déterminant ainsi dans quels cas se produisent des autorisations de transferts de données ou des connexions de fichiers, tout en respectant ce principe.

Dans le cas français, nous observons que les sanctions pénales n'ont été appliquées que dans de très rares cas, et cela sous l'impulsion de la CNIL, qui a préféré généralement agir de façon préventive en évoquant dans ses délibérations la sanction pénale du détournement de finalité. Dans les cas les plus graves, la CNIL a adressé des avertissements aux personnes mises en cause et ce n'est qu'à de très rares occasions qu'elle a saisi la justice de faits relatifs à des cas de détournement de finalité[596].

### 4- La présence permanente de « standards » dans le domaine de la protection des renseignements personnels

Ce que nous avons pu observer grâce à l'utilisation de cette grille fait ressortir quelques constatations utiles pour nous aider à comprendre encore mieux la démarche que les autorités de contrôle ont suivie dans les dossiers reliés à l'application du principe de finalité.

Même si nous avons déjà pu constater l'existence de standards d'origine législative et jurisprudentielle dans ce domaine, l'étude de ces données brutes nous montre de façon très spécifique que cette technique se manifeste pendant toute la démarche de prise de décision.

Après avoir étudié les textes légaux en la matière et la jurisprudence, nous avons voulu mieux comprendre comment l'utilisation de standards peut influencer la recherche de l'équilibre de la balance entre les différents intérêts.

---

[596] Voir à ce sujet cette thèse de doctorat portant sur la matière : P. BLANC-GONNET, préc., note 38, p. 78.

Si nous étudions les dossiers en question, nous observons premièrement que les faits entourant les standards sont vraiment variés, à titre d'exemple nous pouvons citer : l'utilisation de numéros d'assurance sociale pour des fins auxquelles la personne concernée n'a pas consenti, la communication à des tiers de renseignements de nature médicale concernant des employés, l'utilisation et la communication d'images à partir de cameras installées dans les lieux de travail, la communication de données biométriques sans le consentement de la personne concernée et la communication à un tiers de renseignements personnels pour des utilisations secondaires des informations transmises sans le consentement de la personne concernée.

Mais nous retrouvons également très souvent des cas d'utilisation de fichiers constitués dans le cadre d'une « mission de service public » à des fins de communication politique, l'adjonction par le responsable du fichier de commentaires et d'informations sur les personnes – commentaires manifestement excessifs au regard des missions de l'autorité détentrice du traitement –, l'existence d'informations sensibles sur les personnes n'ayant pas de lien direct avec la finalité du traitement et n'étant pas pertinentes par rapport au but poursuivi par le traitement, communication à des tiers de listes complètes reprenant toutes les données personnelles sans le consentement des titulaires des données, partage d'informations entre organismes publics mais également avec des acteurs du secteur privé à des fins de prospection commerciale, entre autres.

Nous observons qu'il s'agit surtout de cas où la personne titulaire des renseignements personnels a constaté que ses informations avaient été transférées à un tiers sans son consentement et dans des cas qui ne sont pas encadrés par la loi.

Nous observons généralement que la CNIL va déterminer que l'on se trouve face à une utilisation de données personnelles constituant un détournement de la finalité et donnant lieu à une sanction pénale à cause du manquement aux obligations découlant de la Loi I et L modifiée.

De plus, nous avons pu constater que les faits invoqués sont vraiment variés et induisent une grande quantité de questions entourant la problématique du consentement, ainsi que sur les modalités de consentement *opt-out* et *opt-in*.

Le concept de consentement est donc intiment relié à celui de la « fin acceptable » dans ces dossiers et devient un élément clé à l'heure de juger si la personne concernée aurait pu s'attendre à ce que ses renseignements personnels puissent être communiqués à des tiers dans les circonstances.
Ainsi, le CPVPC a estimé dans la plupart de ces dossiers que la personne concernée devait être informée sur le partage qui avait été fait de ses informations ainsi que sur les utilisations « secondaires » de ses renseignements personnels.
Disons que le seul fait d'informer la personne concernée, par exemple par des dépliants d'information, n'est pas suffisant à l'heure de juger si une personne a compris les finalités pour lesquelles ses renseignements personnels seront utilisés. Pour reprendre une des expressions utilisées, la personne concernée doit comprendre « raisonnablement » quelle sont les utilisations futures de ses renseignements personnels, utilisations qui doivent être limitées et indiquées clairement.
Encore une fois, une « personne raisonnable » ne peut considérer comme adéquat ou acceptable, laisser trop ouvertes ou vagues, les utilisations futures qui seront faites des renseignements personnels la concernant.

Le CPVPC préconise la création d'une liste fermée nommant les tiers qui auront accès aux renseignements personnels ou, si c'est impossible, signalant au moins le type ou la catégorie à laquelle appartiennent ces tiers ainsi que le rapport qu'ils entretiennent avec l'institution qui gère ces renseignements personnels.
Le CPVPC signale également l'importance de respecter le consentement *opt-out* dès qu'il est exprimé, devant arrêter le partage d'informations avec des tiers et l'utilisation des renseignements personnels sans attendre, pour qu'il soit effectif, le plus tôt possible. De la même façon, même s'il existe un consentement actif, *opt-in*, la clause décrivant les communications à des tiers et les usages futurs des

informations ne sera pas valide si elle est trop vague, trop indéterminée ou pas assez précise.

L'analyse faite grâce à notre grille nous a rapidement aidée à identifier dans ces dossiers des standards pouvant nous intéresser dans le cadre de nos recherches. En effet, dans le cadre des dossiers analysés au CPVPC, nous pouvons faire ressortir une certaine flexibilité de la part des personnes concernées à l'heure de partager leurs renseignements personnels quand il s'agit d'utilisation de ces renseignements personnels pour des finalités reliées à « l'intérêt public », la « santé publique », la « sécurité publique » et bien d'autres domaines qui placent face au droit relatif à la protection des renseignements personnels un intérêt collectif, plutôt qu'un autre droit individuel.

Nous constatons alors qu'il devient facile d'identifier une énorme variété de standards qui se trouvent dans le contexte des dossiers relatifs au principe des « fins acceptables » et qui ont justifié la communication à des tiers des renseignements personnels ainsi que leur utilisation ultérieure à des fins autres que leur finalité initiale.

Nous pouvons citer encore d'autres standards à l'origine de l'utilisation des renseignements personnels, tels que la « surveillance des lieux », la « sécurité des installations et des employés », la « vérification de l'état de santé des employés », le « bon fonctionnement de l'entreprise », « l'intérêt public », la « santé publique » et la « sécurité publique », entre autres.
Ces expressions, assez vagues et floues, doivent être interprétées selon les circonstances et se trouvent parfois à l'origine de la justification de certaines utilisations de renseignements personnels. Nous pouvons citer encore « l'intérêt public », la « lutte contre le fraude », la « simplification des démarches administratives » ou les « missions de contrôle », notions qui, dans les dossiers examinés, entrent en conflit avec le critère du respect de la finalité des renseignements personnels.

En tout cas, il est clair que, dans la plupart de ces dossiers, les intérêts s'opposant au droit à la protection des renseignements personnels que le principe de finalité assure sont également formulés sous forme de standard. Ceci est la preuve d'un dialogue permanent, non seulement entre les standards existant dans la formulation des dispositions de lois relatives au principe de finalité, mais également entre celles-ci et les autres valeurs en conflit avec le droit à la protection des renseignements personnels. Nous constatons alors que cette matière est particulièrement basée sur des standards et sur le dialogue constant entre ceux-ci.

Dans le cadre de notre recherche, nous constatons également la constante utilisation d'autres « sous-standards » trouvant leur origine dans la notion de finalité. Nous observons alors l'émergence de certains sous-standards de natures très variées se trouvant dans les dossiers, tels que la « finalité circonstancielle » de certains traitements.

Le standard de la finalité se partage en d'autres sous-standards tels que les « fins compatibles », les « finalités légitimes » et la « conformité des données aux finalités », entre autres.

Nous retrouvons très régulièrement le standard des « expectatives raisonnables » d'un titulaire d'un droit et nous identifions également des expressions telles que « comprendre raisonnablement », les « attentes raisonnables » ou juste le « raisonnable », comme des paramètres devant être examinés.

Des concepts tels que les « utilisations secondaires », les « usages compatibles », ou en anglais, « *secondary use* », ou « *secondary purpose* » se trouvent également dans ces dossiers.

L'utilisation des mêmes notions pour exprimer des idées parfois différentes, démontre déjà une utilisation aléatoire des concepts, qui ne sont pas toujours tenus comme équivalents, créant une jurisprudence qui n'est pas toujours unitaire.

Le dialogue entre standards et une certaine imbrication que nous avons pu observer dans les dispositions relatives au principe de finalité des textes de loi est lui aussi présent dans ces dossiers. Nous identifions alors une technique équivalente de

raisonnement qui va, dans la plupart des cas, faire opérer deux ou plusieurs standards à chaque occurrence.

Il s'agit principalement d'une dynamique basée sur l'appel d'un standard vers un autre standard. Prenons l'exemple de l'exercice visant à déterminer les « fins compatibles » d'utilisation de données personnelles avec la finalité initiale déclarée du traitement où l'analyse est réalisée en faisant appel à la proportionnalité.

Nous vérifions si les données ne sont pas « excessives » par rapport à la finalité initiale en faisant appel au critère de ce qui est « proportionnel », critère que la doctrine n'a pas hésité à qualifier de standard et qui est également doté d'une grande dose d'indétermination et de flexibilité.

Ce que nous observons alors c'est que la présence des standards et le dialogue existant entre ceux-ci est lisible dans les lois, dans la jurisprudence, ainsi que dans le matériel formant les dossiers étudiés par les autorités de contrôle concernant l'application du principe de finalité.
De plus, ces dossiers nous démontrent que nous assistons à un « jeu de standards » dans la pratique puisque, dans la plupart des cas, les intérêts s'opposant au droit à la protection des renseignements personnels que le principe de finalité assure sont formulés également sous forme de standard.
Ce réseau, fonctionnant grâce à l'interaction entre les différents standards que nous avons reconnus dans la formulation du principe de finalité dans les lois, est également opérationnel dans la recherche de l'équilibre entre les intérêts en conflit dans ces dossiers.

**5- Finalité et proportionnalité**

La « proportionnalité » est un standard qui est très souvent mis en relation avec le principe de finalité. Dans le cadre de nos recherches, il nous semble opportun d'analyser comment le principe de proportionnalité est interprété et défini, afin de

pouvoir comprendre par la suite comment il est appliqué en matière de protection des données personnelles. Le critère de la proportionnalité gravite autour de la finalité et constitue un des pôles les plus importants du réseau de dialogue entre standards qui s'établit en la matière.

Il existe une volonté de réaliser une réflexion confrontée à la pratique de l'application du principe de finalité par l'autorité de contrôle belge[597] de la part de certains experts.
T. Léonard, dans l'examen du travail accompli par l'autorité de contrôle belge, identifie des tendances laissant entrevoir une certain « désordre », ainsi que des avis assez « ambigus » dans l'analyse du principe de finalité. Cet auteur souligne également une identification assez « floue » du principe de finalité et le recours à la technique du renvoi à d'autres principes tels que celui de légalité, licéité, admissibilité et proportionnalité[598].

Le rôle majeur accordé au principe de proportionnalité dans le travail de contrôle accompli par la Commission belge est assez large. Ainsi, cet auteur observe comment la place du principe de proportionnalité, induite du principe de finalité, se manifeste par rapport à la proportionnalité des conditions relatives aux finalités, mais également par rapport à la proportionnalité des conditions relatives aux traitements et, fondamentalement, par rapport à la nécessité du traitement.

Finalement, la proportionnalité est examinée par rapport aux conditions relatives aux données et notamment à la conformité des données aux finalités. Cet auteur observe alors une règle de pondération qui se met en fonctionnement dans un nombre considérable d'avis mais il se demande également sur quoi cette règle porte et quels sont les critères utilisés.

---

[597] Thierry LÉONARD, *Conversations cridiennes autour du principe de finalité*, présentation dans le cadre de la Conférence des 30 ans du CRID, Namur, Belgique, le 22 janvier 2010.
Cet auteur dénonce également une interprétation qui va identifier la légalité du traitement à sa légitimité, tout en accordant à une loi qui autorise un traitement la qualité de « présomption » de la légitimité d'un tel traitement, ce qui pourrait paraître dangereux à première vue.
[598] *Id.*

Il se questionne sur la possibilité que la proportionnalité devienne le « principe légal unique de recherche de solution » et dénonce un flagrant arbitraire dans l'application de ce principe ainsi qu'un manque d'objectivité dans son application tirant son origine de la nécessité de fournir des lignes directrices pour l'application de ce principe dans l'examen relatif à la finalité.

En effet, une des questions les plus complexes entourant la notion de standard est celle qui touche à l'arbitraire et aux critères purement subjectifs qui commanderaient leur application.
S. Van Drooghenbroeck réalise une étude approfondie sur la manière dont le principe de proportionnalité apparaît dans le droit de la Convention européenne des droits de l'homme. Cet auteur affirme que la règle de la proportionnalité impose deux ordres d'exigences. Ainsi, avant de déterminer, dans « l'ordre des fins », l'intérêt qui prévaudra sur l'autre – et nous faisons référence ici au critère de proportionnalité au sens strict –, il va falloir s'assurer dans « l'ordre des moyens » de deux questions.

Ainsi, il faut tenir compte de deux critères : d'une part, celui de l'appropriation, afin de vérifier si le sacrifice de l'un promeut en effet la réalisation de l'autre ; d'autre part, celui de la nécessité, afin de voir si la promotion recherchée ne pourrait pas l'être aussi efficacement au prix d'un sacrifice moindre[599].

Voici l'idée que S. Van Drooghenbroeck avance à cet effet : « la mise en œuvre couplée d'exigences instrumentales (appropriation/nécessité) et axiologiques (proportionnalité au sens strict) serait au demeurant parfaitement logique et gage de rationalité du raisonnement »[600].

[599] Sébastien VAN DROOGHENBROECK, *La proportionnalité dans le droit de la Convention européenne des droits de l'homme, Prendre l'idée simple au sérieux*, Bruxelles, Bruylant, Publ. FUSL, 2001, p. 172. Regarder sur ces deux critères la page 172 et suivantes de cet ouvrage.
[600] *Id.*

Observons l'examen réalisé par la Commission de la protection de la vie privée belge, pour ce qui a trait au respect de la triple exigence relative à la finalité d'un traitement de données personnelles que la loi belge impose. Ainsi, la Commission procède depuis des années à l'examen de l'exigence relative à la « finalité déterminée et explicite », mais également à l'étude de ce qui concerne le besoin d'une « finalité légitime ».

Il est fort intéressant d'observer que, à partir des avis de la Commission belge, l'exigence de légitimité de la finalité du traitement semble soumise à une triple interprétation : la première interprétation assimile la légitimité du traitement à la seule valeur de l'intérêt général qu'il incarne ; la deuxième assimile la légitimité du traitement à la légalité de celui-ci ; et la troisième assimile la légitimité à la proportionnalité de celui-ci[601]. Selon certains auteurs, la première et la seconde des interprétations seraient réductrices d'un examen complet de la législation en la matière et la troisième, souffre des « hésitations et des tergiversations de la Commission »[602].

Pour l'objet qui nous occupe, cette troisième interprétation nous aidera à comprendre comment le critère de la proportionnalité est au centre de la construction de la notion de finalité légitime dans le contexte belge.

Certains auteurs cherchent aujourd'hui à comprendre comment est appliquée la règle de la proportionnalité par les autorités de contrôle de protection des données personnelles.

Ainsi, selon certains, la Commission belge juge la légitimité d'un traitement et l'exigence d'une finalité légitime en appliquant le critère de la proportionnalité, et cela selon la perspective exposée dans l'ouvrage de Van Drooghenbroeck cité précédemment.

Ainsi, il semble que la Commission belge de la protection de la vie privée applique dans ses avis, sans les nommer en tant que telles, certaines exigences substantielles et formelles du critère de proportionnalité.

---

[601] E. DEGRAVE, préc., note 582, 53 et 54.
[602] *Id.*, 54.

Les exigences substantielles visant le « contenu » de la mesure qui limite la vie privée sont importantes et par conséquent il est essentiel de respecter les critères d'appropriation, de nécessité et de proportionnalité au sens strict.

Toutefois, des exigences plutôt « formelles » visent à vérifier le respect des règles formelles et procédurales et mettent l'accent « non plus sur le *contenu* du *juste équilibre* à réaliser, mais bien sur la *manière* de le réaliser, en termes de processus décisionnels »[603].

Alors, dans le contexte de la protection des données personnelles et si l'on pense à la vérification du respect de ces exigences par l'autorité de contrôle, le critère d'appropriation consiste à voir si la mesure créant la limitation du droit à la vie privée est suffisamment énergique pour atteindre l'objectif visé.

Le critère de nécessité impose de vérifier s'il n'existe pas une mesure moins liberticide que celle qui a été retenue, qui pourrait permettre également d'atteindre l'objectif visé[604].

Mais il faudra encore examiner la proportionnalité au sens strict, ce qui « se révèle délicat en pratique »[605]. Pour certains, il faut se demander dans un premier moment, si l'on doit nécessairement placer dans la balance la limitation du droit à la vie privée des personnes concernées face à l'intérêt général ou, si l'on peut faire valoir des intérêts individuels. Toutefois, les difficultés ne s'arrêtent pas ici : « une fois identifiés les intérêts à mettre en balance, l'évaluation de l'équilibre existant – ou non – entre eux n'est pas moins complexe »[606], puisqu'on « cherche à mesurer des intérêts incommensurables »[607].

La Commission belge réalise également un examen des exigences formelles du critère de proportionnalité, « qui semblent pouvoir compenser, partiellement du moins, la subjectivité dont est empreinte l'appréciation des exigences substantielles de proportionnalité, en permettant aux personnes concernées d'exercer elles-mêmes

[603] *Id.*, 56.
[604] Voir sur ces deux critères : *Id.*
[605] *Id.*, 58.
[606] *Id.*, 59.
[607] *Id.*

un certain contrôle de l'utilisation de leurs données ou en confiant ce rôle à une autorité chargé de se prononcer concrètement au cas par cas »[608].

**6- Les autorités de contrôle, pondération des intérêts et standards**

Si nous regardons maintenant le travail qui est réalisé par ces acteurs interprètes des principes de protection des renseignements personnels, nous arrivons à comprendre que le mécanisme habituel qui se déclenche lors de la recherche de l'équilibre reste assez complexe. Ce *balancing test*[609], si nous voulons adopter l'expression américaine, est pour certains assez illusoire puisqu'au terme de cette recherche d'équilibre, un intérêt ou une liberté fait nécessairement céder l'autre[610].

Dans les termes utilisés par F. Rigaux, dans les cas où deux libertés fondamentales vont entrer en conflit, la recherche d'une solution passe par la tentative de les ajuster l'une à l'autre, avec l'objectif d'aboutir à l'élaboration d'une règle nouvelle, capable de justifier la décision finale retenue.

Nous notons que le juge, mais aussi l'autorité de contrôle, va devoir finalement choisir entre les deux parties, celle qui se prévaut du droit à la vie privée et celle qui avance pour sa défense l'exercice d'une autre liberté ou la défense d'un intérêt légitime et, toujours l'une aux dépens de l'autre[611].

Toutefois, comme F. Rigaux l'a souligné, « seule la méthode de pondération des intérêts (...) permet de dénouer le conflit entre deux libertés ou le conflit entre une liberté et l'intérêt général »[612].

---

[608] *Id.*, 62.

[609] Cette expression a été reprise par le professeur François Rigaux : F. RIGAUX, préc., note 587, p. 47.

[610] François RIGAUX, « Les paradoxes de la protection de la vie privée », dans Pierre TABATONI (dir.), *La protection de la vie privée dans la société de l'information*, Tome I, Paris, P.U.F., 2000, p. 9.
F. Rigaux avance les expressions utilisées dans la doctrine américaine et allemande pour désigner cet exercice cherchant l'équilibre, qu'il considère illusoire.

[611] *Id.*

[612] François RIGAUX, « La doctrine des droits de la personnalité », dans François RIGAUX (dir.), *La vie privée, une liberté parmi les autres?*, Travaux de la Faculté de droit de Namur, t. 17, Bruxelles, Larcier, 1992, 116, p. 137.

Nous avons eu l'occasion de constater que le législateur communautaire, à l'heure de légiférer en la matière, a eu recours à des concepts plutôt indéterminés et à des normes conditionnelles. Pour ce qui est du droit canadien en la matière, cette tendance se confirme d'une certaine manière.

Certains vont encore plus loin dans l'analyse des dispositions en la matière, en affirmant que l'ambivalence des objectifs, qui sont plus contradictoires que complémentaires, entraîne des hésitations « dans la rédaction des textes et l'accumulation d'incertitudes qui vont au-delà du recours occasionnel à des concepts indéterminés »[613]. En effet, les incertitudes des textes en la matière laissent une grande place à l'interprétation des autorités de contrôle qui vont jouer un rôle important dans l'exercice de décodage des concepts indéterminés présents dans les lois.

Prenons l'exemple de la Directive 95/46/CE, analysée dans les lignes précédentes, pour expliquer à quel exercice doivent se livrer les autorités de contrôle, surtout dans le contexte européen, mais également dans le cas du Canada.

Pour F. Rigaux, il est douteux qu'un législateur soit en mesure de préciser la portée d'un texte aussi vague, qui se limite exclusivement à poser les problèmes sans y apporter aucune solution. Cet auteur affirme qu'il appartiendra sans doute aux autorités de contrôle nationales et communautaires principalement, mais aussi le cas échéant aux cours et tribunaux de se prononcer sur l'interprétation des textes en la matière à la lumière des cas concrets et des litiges particuliers qui leur seront soumis[614].

Toutefois, l'exercice est complexe, en partie à cause des dispositions qui encadrent cette matière. Prenons comme exemple une disposition de la Directive 95/46/CE qui met en balance non seulement une, mais deux notions indéterminées.

---

[613] François RIGAUX, « Libre circulation des données et protection de la vie privée dans l'espace européen », dans Pierre TABATONI (dir.), *La protection de la vie privée dans la société de l'information*, Tome II, Paris, P.U.F., 2000, 25, p. 29.

[614] Voir à ce sujet : *Id.*, p. 30.

Ainsi, le paragraphe 7(f) de la Directive 95/46/CE présente, d'une part, un « intérêt légitime » et, d'autre part, le « seul principe du droit au respect de la vie privée » ! Comme certains auteurs l'ont signalé, on aurait pu s'attendre plutôt à ce que le législateur fasse une distinction entre ce qui est légitime et ce qui ne l'est pas[615], mais en tout cas des dispositions de cette nature nous montrent l'esprit des législations en la matière où, une fois encore, nous constatons la présence de nombreux standards. Nous avons pu étudier dans les lignes précédentes que cette tendance est observable dans l'articulation des textes en la matière.

Mais l'abandon de la part du législateur des techniques classiques pour légiférer, ne s'arrête pas ici puisque, pour certains, le législateur a également abandonné les modes traditionnels de règlement de conflits en ayant recours aux autorités de contrôle aptes « à évaluer avec souplesse des intérêts conflictuels »[616]. Le rôle de ces autorités de contrôle en tant qu'interprètes prouve également que l'autorité judiciaire dans ce contexte s'est vu réduire son rôle traditionnel d'arbitre en cas de conflit.

Y. Poullet et T. Léonard se demandent dès 1992, d'une part, sur quelle base les autorités de contrôle et, le cas échéant, le juge vont pouvoir garantir et contrôler rationnellement une pondération d'intérêts permettant l'éclosion du marché de l'information fondé sur la libre circulation des données et la protection des libertés individuelles[617].

En sachant que cet arbitrage s'opère uniquement à propos de situations particulières, toujours spécifiques, ils cherchent à savoir si une « règle méthodologique » ou une « méthode » générale permettant aux autorités de contrôle d'exercer leurs missions avec rigueur et transparence ne peut pas être dégagée. Poullet et Léonard indiquent sans hésiter la thèse de F. Rigaux comme pouvant nous conduire à cette méthodologie.

---

[615] *Id.*
[616] F. RIGAUX, prec., note 610, p. 38.
[617] Y. POULLET et T. LÉONARD, préc., note 30, p. 244.

Ainsi, le conflit d'intérêts ou des libertés doit se résoudre par la « Méthode de pondération des intérêts », par laquelle l'autorité chargée de trancher le conflit appréciera les intérêts légitimes respectifs propres à chaque partie exprimant sa liberté »[618]. Certains se demandent s'il existe un débat entre deux libertés : celle du ficheur et celle du fiché. Toutefois, ce débat ne pouvant pas se résoudre une fois pour toutes exige que l'autorité chargée d'arbitrer ce débat puisse peser les intérêts en jeu, et ce « au regard d'une évolution technologique qui interdit de figer les solutions mais oblige à apprécier combien celle-ci modifie les équilibres fragiles à peine définis »[619].

F. Rigaux préconise l'application de la « méthode » de la pondération des intérêts afin, d'une part, de résoudre un conflit opposant deux libertés fondamentales, en aidant à soupeser les intérêts en cours, et, d'autre part, d'aider à la résolution d'un conflit entre une liberté fondamentale et un intérêt général, « en évaluant la restriction qui peut être apportée à une liberté individuelle en raison d'une nécessité sociale » [620], ce qui pourrait trouver son application dans le contexte du secteur public et de l'administration électronique en particulier.

Nous considérons également que tout va dépendre du caractère plus ou moins ouvert que, dans le contexte juridique particulier, l'on accorde à des concepts tels que « l'intérêt général », laissant la possibilité d'interpréter de tels concepts au cas par cas.

Nous pouvons imaginer deux situations de conflit entre deux libertés, qui se présente quand l'État restreint l'une d'elles ou quand la concurrence s'établit entre des libertés différentes que les citoyens font valoir l'une contre l'autre.
Certains affirment que c'est uniquement dans le terrain de l'opposition binaire privé-public qu'il y a une possible intervention de « l'authentique

[618] *Id., p.* 20.
[619] *Id.*,p. 250.
[620] *Id.*, p. 251.

proportionnalité »[621], appliquée dans la recherche de l'équilibre entre l'intérêt général de la communauté et le respect des droits fondamentaux de l'individu.

Toutefois, F. Rigaux signale que, dans les deux cas, la décision du juge repose sur ce que requiert « l'intérêt général », raison pour laquelle la Cour suprême des États-Unis préfère généralement une « méthode abstraite ou générale de pondération des intérêts » (*categorical balance*) à l'évaluation de ceux-ci « cas par cas » (*ad hoc balancing test*)[622].

Par contre, pour ce qui est de la Cour européenne des droits de l'homme, il paraît clair que la Cour a fait un véritable choix et qu'elle applique un contrôle concret et un *ad hoc balancing* dans l'exercice de sa juridiction, et cela pour une raison très concrète : « la justice des droits de l'Homme n'est pas décernée et recherchée dans les choix normatifs, généraux et abstraits, et dans les situations typées et standardisées, mais bien dans la concrétude des situations particulières affectées par tels choix »[623].

B. Docquir signale en 2008 que, dans les arrêts les plus récents de la Cour européenne des droits de l'homme, il observe une tendance à substituer « l'analyse classique du critère de la proportionnalité » par la recherche du « juste équilibre » entre les intérêts en présence, y compris dans les hypothèses où l'ingérence reprochée est le fait de l'État et non d'un particulier[624].

Il faut noter que, dans cette matière, cette Cour suit une approche plutôt casuistique : ainsi, dans certains cas, elle va refuser de faire prévaloir un intérêt sur l'autre de façon générale et elle va par contre apprécier finement et de façon *ad hoc*

---

[621] Voir à cet effet : S. VAN DROOGHENBROECK, préc., note 621 ,p. 247.
[622] François RIGAUX, « Le droit entre un en déça et un au delà », dans François RIGAUX (dir.), *La vie privée, une liberté parmi les autres?*, Travaux de la Faculté de droit de Namur, t. 17, Bruxelles, Larcier, 1992, 161, p. 223.
[623] S. VAN DROOGHENBROECK, préc., note 621, p. 255.
[624] Benjamin DACQUIR, « Le droit de la vie privée : aperçu général et règle de la proportionnalité », dans Benjamin DACQUIR et Andrée PUTTEMANS (dir.), *Actualités du droit de la vie privée*, Bruxelles, Bruylant, 2008, p. 27.

l'ensemble des circonstances de l'espèce pour chercher à savoir si ce « juste équilibre » a été préservé sur le plan matériel et procédural[625].
Pour cet auteur, « l'ampleur des enseignements doctrinaux sur l'interprétation de la règle de la proportionnalité est parfois directement proportionnelle à l'embarras du praticien chargé de l'appliquer pour conseiller ou pour juger »[626].

Comme S. Van Drooghenbroeck l'a signalé, appliqués à une même affaire, *ad hoc balancing* et *categorical balancing* pourraient conduire à des conclusions opposées. Il nous rappelle également que si un juge pratique au cas par cas et sans justification convaincante, tantôt un *ad hoc balancing*, tantôt un *categorical balancing*, un certain soupçon de partialité pourrait peser sur lui[627].

Il nous semble que, d'une manière générale, les autorités de contrôle appliquent les principes de protection des renseignements personnels plutôt au cas par cas, puisqu'elles réalisent l'exercice de pondération pour chaque situation de conflit qui se présente en adoptant plutôt un exercice comportant le modèle de l'*ad hoc balancing.*

Il nous paraît pourtant clair que « pondérer les intérêts est un exercice périlleux dès lors qu'aucune démarche systématique n'est proposée au juge ou à l'autorité de contrôle afin de guider leur raisonnement »[628]. Il est essentiel de munir le juge et l'autorité de contrôle de certains critères permettant d'assurer par la suite une démarche rationnelle, l'atteinte d'un équilibre entre les libertés et intérêts en question.

Selon Poullet et Léonard, en appliquant la « Règle de la proportionnalité » dans la démarche visant à trouver l'équilibre, on pourra fixer des limites au pouvoir d'appréciation de ceux qui ont pour mission d'appliquer le principe de finalité.

---

[625] *Id.*
[626] *Id.*, p. 28.
[627] Voir à ce sujet : S. VAN DROOGHENBROECK, préc., note 621, p. 251 et 252.
[628] Y. POULLET et T. LÉONARD, préc., note 30, p. 252.

En plus, dans le contexte de la protection des renseignements personnels, tellement changeant et en pleine évolution technologique, « d'une certaine manière, la proportionnalité s'impose comme l'outil *tout terrain* que réclame un souci d'adaptation aux changements de circonstances »[629].
Ces auteurs dégagent une piste de solution dans la possible application de la règle de la proportionnalité au contrôle de la finalité. Voici comment ces auteurs expliquent en quoi consiste cette règle, dotée d'une grande souplesse qui permet son utilisation dans un nombre infini d'hypothèses.

Cette règle comporte un triple examen : le premier porte sur le contrôle de « l'utilité » de l'acte ou des moyens mis en œuvre ; le second vise plutôt le « caractère indispensable » des mesures adoptées ou envisagées, afin de vérifier qu'elles ne peuvent pas être remplacées par d'autres mesures permettant d'atteindre le même objectif, avec une efficacité identique, mais en étant plus respectueuses de la liberté ou de l'intérêt en jeu ; et finalement, le troisième vise à s'assurer que l'atteinte des libertés par les mesures adoptées n'est pas « disproportionnée » par rapport au but poursuivi[630].

Pour ce qui est du respect de cette règle dans le contexte du secteur public, F. Rigaux présente les conditions devant être retenues afin de voir si l'État respecte le principe de proportionnalité : l'État va pouvoir restreindre l'exercice d'un droit en raison d'un intérêt légitime et contraignant si les conditions sont énoncées en termes généraux, sans qu'il y ait d'application discrétionnaire à un cas particulier et si, parmi les mesures restrictives qui sont à sa disposition, il choisit celle qui pénètre le moins profondément dans la sphère de liberté du sujet.

Pour F. Rigaux, il appartient au juge de contrôler le respect par les organes de l'État des libertés individuelles et d'appliquer la méthode de la pondération des intérêts,

[629] S. VAN DROOGHENBROECK, préc., note 621, p. 164.
[630] Il faut noter que Poullet et Léonard nous rappellent que si les droits ou libertés en conflit sont protégés par des normes de hiérarchie égales, l'application de la règle de la proportionnalité va prolonger le principe selon lequel l'exercice d'un droit ou d'une liberté trouve sa limite dans celui ou celle qui est exercé par autrui.

*Balancing test* ou *Interessenabwägung*[631]. Cette démarche convient également aux autorités de contrôle dans leur rôle de décideur, grâce à la méthode de pondération des intérêts.

Notons que la règle de la proportionnalité diffère de la pondération des intérêts, puisqu'elle guide le raisonnement de celui qui cherche à vérifier si l'équilibre des intérêts est respecté. Ainsi, la méthode de la pondération des intérêts « consiste en une application de la règle de la proportionnalité en vue de cerner l'équilibre à atteindre »[632].

Pour certains, les avantages de cette méthode de pondération des intérêts sont nombreux : elle est systématique, complète, elle permet au raisonnement d'acquérir une assise méthodologique, elle va accorder au jugement de valeur posé par l'autorité de contrôle un degré de transparence capable de réduire l'indétermination de la pondération en tant que telle et, finalement, elle fait diminuer le risque de subjectivité en accordant au processus décisionnel une transparence qui est un gage de confiance.

Toutefois, dans la pratique, nous observons qu'en réalité cette règle ne s'applique pas tout à fait d'une façon aussi « méthodologique » et ordonnée. Nous nous demandons si, en réalité, il existe une certaine absence de « méthode » à l'heure de l'appliquer dans le travail quotidien des décideurs dans la matière.

Nous observons également dans le contexte canadien qu'un critère méthodologique peut être d'application à l'heure de déterminer si la violation d'un droit de la Charte canadienne des droits et libertés est justifiée dans une société libre et démocratique. Il s'agit du Critère Oakes, qui émane de l'arrêt de la Cour suprême du Canada R.c. Oakes[633].

[631] F. RIGAUX, préc., note 622, p. 222 et 223.
[632] Y. POULLET et T. LÉONARD, préc., note 30, p. 255.
[633] R. c. Oakes [1986] 1 R.C.S. 103.

Le CPVPC, dans un document portant sur les mesures de sécurité, parle de certains facteurs devant être pris en considération à chacune des étapes afin de veiller à ce que la vie privée soit respectée dans le contexte de la mise en œuvre de programmes et de politiques touchant à la sécurité[634].

Dans une première étape, celle de la « conception », le CPVPC préconise l'application du Critère Oakes qui fournit un cadre pouvant servir à l'analyse de la viabilité d'une initiative en matière de sécurité, « bien qu'il ait été conçu pour déterminer si une apparence de violation de la Charte est justifiée en application de l'article 1 de celle-ci »[635].

Ce Critère Oakes exige quatre conditions : la nécessité, la proportionnalité, l'efficacité et une intrusion minimale.

Ainsi, il faut qu'il existe une « nécessité clairement définie, liée à une préoccupation sociétale pressante »[636] que l'on voudrait régler pour la mise en place d'une telle mesure.

De plus, la mesure en question « doit être minutieusement ciblée et personnalisée afin d'être raisonnablement proportionnelle à l'atteinte à la vie privée »[637].

Par la suite, il s'agit de démontrer que la mesure est « empiriquement efficace en vue de régler le problème et être clairement associée à la résolution du problème »[638].

Nous considérons comme particulièrement importante cette évaluation « empirique », qui doit être faite en vue de déterminer l'efficacité de telles mesures, obligeant à effectuer une « vraie » évaluation s'appuyant sur des critères purement empiriques. Pour finir, et afin de garantir une intrusion minimale, la mesure doit

---

[634] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle*, Document de référence, Novembre 2010.
[635] *Id.*, p. 11.
[636] *Id.*
[637] *Id.*
[638] *Id.*

être l'option la moins envahissante en s'assurant que « toutes les autres options d'enquête moins envahissantes ont été épuisées »[639].

Nous constatons que ces critères, répondant à des notions qui elles-mêmes répondent aux caractéristiques des standards et ayant la proportionnalité comme une des notions-clés, doivent être appréciés dans leur ensemble et comme un « tout », puisqu'ils constituent une « méthodologie » capable de fournir un cadre d'analyse.
C'est à notre avis un bel exemple d'outil capable d'aider à déterminer l'impact de certaines mesures pouvant limiter le droit à la vie privée.
L'éventuelle application de ce critère dans le cadre de l'adoption des mesures de sécurité témoigne du potentiel d'application à toute autre circonstance afin de mesurer l'impact de tout programme ayant une incidence sur le respect du droit à la protection de la vie privée.

Examinons maintenant comment, par le biais du principe de finalité, la méthode de pondération des intérêts est mise en œuvre dans le contexte du droit à la protection des renseignements personnels. Si nous analysons les dispositions faisant référence au principe de finalité que nous avons analysé dans les pages précédentes, nous constatons que toute finalité n'est pas acceptable et qu'un examen au cas par cas s'impose.

**7- Principe de proportionnalité et administration électronique**

Ainsi, d'une part, les données doivent être enregistrées pour des finalités déterminées et légitimes, obligation qui pose le « principe de légitimité ». D'autre part, les données doivent être pertinentes, adéquates et non excessives par rapport à la finalité légitimement déterminée, obligation qui pose le « principe de conformité ». Le problème est alors de cerner la portée exacte du principe de finalité qui est un double principe : légitimité d'une part et conformité d'autre part.

[639] *Id.*

Pour certains, la méthode de pondération des intérêts va être capable d'offrir aux autorités de contrôle des critères d'évaluation permettant de donner un contour plus précis aux principes de légitimité et de conformité[640].

Toutefois, même si les principes de légitimité et de conformité participent à la recherche de l'équilibre, nous observons qu'ils diffèrent dans leur contenu. Ainsi, si nous voulons circonscrire les finalités légitimes d'un traitement, certains affirment qu'il faut absolument respecter deux règles qui ont trait au principe de légitimité.

Nous observons alors une règle « formelle », qui est sans rapport avec le choix effectué par le responsable du traitement et qui oblige à ce que les finalités soient définies de manière claire et précise et qui demande de la désignation d'un responsable du traitement.
Mais nous identifions également une règle de « fond », celle où la méthode de la pondération des intérêts va pouvoir à s'appliquer : selon cette règle, le choix de la finalité s'effectue dans le respect du point d'équilibre entre l'intérêt du responsable du traitement et les intérêts des personnes concernées par les données.

Pour ce qui est du principe de conformité, il va appeler clairement l'application de la méthode de pondération. Selon Poullet et Léonard, les trois critères retenus concernant ce principe – l'adéquation, la pertinence et le caractère non excessif – correspondent exactement au triple examen propre à la règle de la proportionnalité : utilité, nécessité et proportionnalité.
Nous identifions également les conditions du Critère Oakes, applicable au contexte canadien : la nécessité, la proportionnalité, l'efficacité et une intrusion minimale.

Nous notons alors que la pondération doit se réaliser non pas lors du choix de la finalité mais plutôt lors de la sélection des données qui vont être traitées. Ce qui implique que le contrôle de la finalité se réalise grâce à un double contrôle portant

[640] Y. POULLET et T. LÉONARD, préc., note 30, p. 257.

sur la légitimité des finalités et sur la conformité des données avec la réalisation de ces finalités[641].

Ainsi, dans le contexte du secteur public, la finalité du traitement sera « légitime » si elle respecte le principe de légalité, afin de garantir le respect de la règle formelle. Mais il faudra également répondre aux principes de spécialité et de proportionnalité, afin de garantir que la règle de fond soit l'équilibre des intérêts.

Notons que le contrôle de légitimité par la méthode de pondération est vraiment bien adaptée au secteur public, et cela grâce au fait que les principes de « spécialité » et de « proportionnalité », qui sont à la base de toute l'action administrative, se confondent dans ce contexte avec la règle de la proportionnalité.
Pour ce qui est du contrôle de la conformité, il est signalé par ces auteurs que, pour que le traitement d'une donnée personnelle puisse répondre à ce principe, il y a trois conditions à respecter : l'adéquation, la pertinence et le caractère non excessif par rapport à la finalité du traitement dont il fera l'objet[642].

C.-A. Morand souligne que les principes directeurs vont permettre de favoriser « l'inter normativité croisée » entre les valeurs et intérêts que nous retrouvons dans le cadre des politiques publiques et ceux qui vont se retrouver plutôt dans d'autres réseaux normatifs, tels que les droits fondamentaux.

Pour cet auteur, le principe de proportionnalité est celui qui est appelé à réaliser le mieux cet exercice : « Parmi les liens qui se tissent entre ces deux territoires normatifs, le principe de proportionnalité joue un rôle primordial dans ses trois composantes : le principe relatif à l'aptitude d'une mesure à atteindre les objectifs

[641] *Id.*, p. 259 et 260.
[642] Poullet et Léonard ajoutent que l'adéquation et la pertinence doivent se comprendre dans ce contexte comme impliquant une liaison nécessaire et suffisante de la donnée ou de la catégorie des données avec la finalité en cause.

poursuivis, celui qui porte sur le caractère nécessaire de la mesure envisagée et celui qui a trait à la subsidiarité de celle-ci »[643].

Nous considérons que ce principe va pouvoir aider à l'heure de mesurer les possibles limitations du droit à la protection des données personnelles dans le contexte de la mise en place de certaines prestations électroniques de services propres à l'administration électronique. En effet, les besoins de l'administration pour accroître l'efficacité administrative ou pour permettre un meilleur fonctionnement de l'appareil étatique peuvent être à l'origine de l'établissement de certains programmes pouvant avoir des incidences sur le droit à la protection de la vie privée. Nous pouvons imaginer alors le recours au principe de proportionnalité dans le processus d'évaluation de l'impact que de telles mesures peuvent avoir sur ce droit fondamental.

Cet auteur établit trois composantes de ce principe afin d'évaluer l'impact de certaines mesures pouvant être adoptées dans le cadre d'une politique publique, et que nous allons tenter d'appliquer dans le cadre de la mise en place des services propres à l'administration électronique.

Tout d'abord, le principe d'aptitude permet de s'assurer que les restrictions du droit à la protection des renseignements personnels concourent effectivement, et non pas de manière supposée, à la réalisation d'une politique publique dans ce cas relative à la mise en place de l'administration électronique.

Ensuite, le principe de « nécessité » va nous aider à constater que l'objectif recherché ne pouvait pas être atteint par des mesures moins restrictives pour le droit à la protection des renseignements personnels.

Finalement, le principe de « subsidiarité », de proportionnalité au sens étroit, va permettre de vérifier qu'un « rapport raisonnable »[644] est établi entre la gravité des effets produits par une mesure restrictive sur la situation de l'administré et l'objectif visé par la politique publique en question.

---

[643] C.-A. MORAND, préc., note 19, p. 191.

[644] *Id.* Cette expression littérale est utilisée par cet auteur.

Notons que, pour vérifier la dernière des trois composantes du principe de proportionnalité, l'exercice se base sur le renvoi vers le critère du « raisonnable », ce qui démontre que, même en suivant cette méthodologie pour l'appréciation des limitations des droits fondamentaux, nous sommes encore face à une complexité dans l'appréciation qui tire son origine du perpétuel renvoi d'une notion vers l'autre.

En effet, ce rapport raisonnable pourra faire l'objet d'interprétations multiples, pouvant donner lieu à des solutions assez différentes.
Cette difficulté n'a pas échappé à l'auteur, qui souligne également la complexité dérivant des législations basées sur des « principes » : « Ces trois sous-principes génèrent des décisions d'autant plus complexes qu'ils postulent des jugements de conformité avec des législations qui elles-mêmes fonctionnent à l'aide de principes et dont les effets restent dès lors longtemps virtuels »[645].

En effet, les difficultés que pose la nature même de ces législations, articulées sur la base des principes ou des « standards », a un impact sur les décisions auxquelles on peut aboutir grâce aux trois composantes du principe de proportionnalité. Pensons alors tout d'abord à la manière dont les législations en matière de protection des données personnelles s'articulent autour d'un ensemble de principes, tels que celui de finalité, légitimité et qualité des données entre autres. Dans un deuxième temps, observons que, dans les textes de loi encadrant le fonctionnement des services publics offerts par l'administration, des notions telles que la « qualité des services »[646] ou « l'efficacité administrative » se trouvent également au cœur de ces législations. Cette tendance se confirme si nous étudions les nouvelles législations encadrant l'administration électronique, législations qui ont été adoptées dans plusieurs pays.

[645] *Id.*
[646] L. CLUZEL-MÉTAYER, préc., note 181.

Nous constatons alors que la complexité dont C.-A. Morand parle garde toute son actualité dans les cas qui nous occupent dans le cadre de nos recherches.

Nous observons que, d'après les analyses de certains experts belges, l'autorité de contrôle belge procède à l'application du principe de finalité à l'heure de prendre une décision sur les équilibres à préserver entre les différents droits en tension. La CNIL a expliqué à plusieurs reprises que ce principe est d'application dans certains dossiers et dans son travail d'interprétation en général.

Regardons par exemple les questions entourant l'installation de caméras de vidéosurveillance, matière qui touche à l'exercice des libertés publiques et, principalement, la liberté fondamentale d'aller et de venir, raison pour laquelle le principe de proportionnalité constitue la principale garantie.

Ainsi, pour ce qui est de l'utilisation de cette technologie, la CNIL « après avoir rappelé le principe de proportionnalité, a formé le vœu qu'il ne soit recouru aux dispositions de vidéosurveillance que dans les cas où ils constituent une mesure adéquate, pertinente et non excessive au regard de la finalité telle qu'elle est portée à la connaissance du public »[647].

Regardons également que dans les cas d'interconnexions entre fichiers, la CNIL procède à plusieurs analyses portant sur l'absence de contradiction entre « le projet et l'encadrement juridique existant (notamment au regard des règles sur le secret professionnel), les finalités recherchées (et tout particulièrement la proportionnalité des moyens mis en œuvre au regard des objectifs poursuivis), la pertinence des informations mises en relation, la liste des bénéficiaires des nouveaux circuits d'information qui en résultent, ainsi que les modalités d'information des personnes concernées par l'interconnexion »[648].

[647] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, préc., note 171, p. 100 et 101 (nous soulignons).
[648] *Id.*, p. 172 (nous soulignons).

Nous pensons que c'est en effet l'idée que Poullet et Léonard défendent par rapport à la thèse de F. Rigaux, celle qui apporte un éclairage sur cette complexité du droit à la protection de la vie privée que nous observons aujourd'hui :

> « La thèse de M. Rigaux abolit définitivement toute idée d'une "vie privée" en soi aux contours définis et conçue sur le mode d'une propriété. Elle invite à un débat plus essentiel, plus complexe et plus vivant qui renvoie la question de la protection des données à un nécessaire arbitrage entre libertés. En quittant le domaine de la propriété le débat sur la protection des données a perdu certitudes, celle d'une vie privée bien circonscrite, celle de finalités décrites une fois pour toutes ; en rentrant dans le domaine des libertés, elle a gagné en inquiétudes, non celles, paralysantes, conduisant au refus du progrès technique, mais bien celles, mobilisatrices, invitant à entamer en des lieux divers une discussion fondée sur la transparence des enjeux de la technologie informationnelle, et ce, afin que s'élaborent de véritables choix. »[649]

Cette approche préconisée par F. Rigaux sur les questions relatives au droit à la protection de la vie privée nous permet de cerner cette complexité que nous constatons à l'heure d'examiner comment le principe de proportionnalité trouve son application dans le domaine de l'administration électronique.

[649] Y. POULLET et T. LÉONARD, préc., note 30, p. 275 et 276 (nous soulignons).

**PARTIE 2 : Le principe de finalité comme instrument de gouvernance des réseaux en vue de protéger les renseignements personnels**

## CHAPITRE 1 LA CIRCULATION DES RENSEIGNEMENTS PERSONNELS DANS LE MODÈLE DU SILO ET LES MÉCANISMES D'ADAPTATION « RÉSEAUTIQUE »

Nous analyserons dans ce chapitre quel est aujourd'hui le modèle de partage des informations entre deux ou plusieurs entités du secteur public. Il s'agira d'observer si les modes de circulation et de partage des informations correspondent habituellement à une logique de structure en silo.

Toutefois, ces modes de circulation et de partage ont lieu dans des structures assez variées, puisque nous pouvons identifier notamment des structures en silo, mais encore d'autres structures, qui subissent aujourd'hui une métamorphose provoquant le passage d'un modèle en silo vers un modèle en réseau.

Ces modes de circulation ont également lieu dans des structures qui conforment totalement ou partiellement de véritables structures en réseau. Dans tous les cas, nous observons que ces modes de circulation ne sont pas les plus adaptés aux structures en réseau, puisqu'ils sont basés fondamentalement sur des structures où les interconnexions et le partage d'informations sont « étrangers » à un tel modèle.

De plus, si les modes de circulation ne sont pas adaptés au modèle du réseau, les règles et les mécanismes conformant le cadre de gouvernance de ces flux d'information ne sont pas les plus adéquats.

Nous examinerons quels sont les possibles obstacles que nous identifions aujourd'hui à l'encadrement correct de ce nouveau modèle d'administration, et cela afin de pouvoir compter sur des instruments de gouvernance adaptés à des structures où les informations circulent de plus en plus et où les renseignements personnels ont tendance à être partagés dans un modèle de circulation en réseau.

## SECTION 1 Le modèle de partage aujourd'hui : un cadre basé sur l'exception

Regardons maintenant comment se présente le cadre permettant le partage des informations entre les organismes du secteur public aujourd'hui. Cette analyse va nous aider à identifier les mécanismes qui encadrent la circulation des renseignements personnels, ainsi que les limites d'un tel modèle.
En effet, le modèle actuel est basé plutôt sur une « liste d'exceptions » permettant de contourner la règle générale, qui préconise de limiter la circulation des informations et qui a été fondamentalement conçue pour encadrer le modèle en silo.

### 1- Contournement de la règle générale par un catalogue d'exceptions

Nous avons pu observer dans les pages précédentes que le cadre s'appliquant à la circulation des renseignements personnels et à leur échange entre organismes appartenant au secteur public au Canada et en Europe s'appuie sur un régime à caractère général.
Ainsi, nous avons observé que les systèmes de protection des renseignements personnels sont présidés par des principes qui établissent la règle du « non-partage » des informations entre organismes, et cela en grande partie à cause de la forme même de la structure permettant la circulation des renseignements qui favorise particulièrement l'étanchéité des fichiers.

Ainsi, par le passé, l'idée des bases de données structurées en silos, séparées, indépendantes et encadrées par le principe de finalité qui limitait notamment leur interconnexion a clairement commandé les mouvements d'information au sein du secteur public.

La règle générale préconise que les renseignements personnels ne soient pas communiqués à autrui, ni utilisés à des finalités autres que celles qui ont été spécifiées au moment de la collecte ou pour des finalités compatibles avec celles-ci,

sauf si la personne concernée a pu manifester son consentement ou si une règle de droit le permet.

Nous observons alors une règle générale qui exige le respect des principes faisant référence à la confidentialité des renseignements personnels, à la non-communication de ces renseignements à autrui, et ce même pour des fins compatibles, et finalement la non-utilisation des renseignements recueillis contraire aux finalités qui ont motivé leur traitement.

Cette règle générale est basée également sur le recours au mécanisme du consentement de la personne concernée pour autoriser la communication des renseignements les concernant, mécanisme qui commande clairement les modalités de partage des informations de façon générale.
Toutefois, nous remarquons très clairement que ce cadre est également basé sur une certaine facilité à contourner la règle générale. Il est intéressant d'observer les articles – comportant normalement une longue liste d'exceptions – qui permettent la communication et l'usage des renseignements, et cela sans le consentement de la personne concernée.

Nous avons pu constater également dans les pages précédentes que l'on trouve des exceptions dans les lois, afin de permettre l'interconnexion de certaines bases de données sous des conditions *a priori* très strictes et balisées.
De la même manière, nous avons pu identifier de « vraies passoires » en analysant les dispositions permettant la communication de renseignements personnels entre organismes du secteur public, qui gardent la possibilité de communiquer ces renseignements au cas où les autorités administratives pourraient en avoir besoin et cela sans le consentement des personnes concernées[650], ce qui peut poser des problèmes importants dans le domaine de la maîtrise des renseignements personnels.

[650] Nous pouvons penser notamment à l'alinéa 8(2) de la LPRP canadienne, qui s'applique aux renseignements rélevant d'une institution fédérale.

Nous observons alors que, depuis quelques années, nous assistons à la mise en place d'un « catalogue d'exceptions », autorisant à contourner la règle générale, afin de permettre la communication des renseignements personnels par les organismes du secteur public.
De plus, des textes applicables à des secteurs particuliers vont mettre en place des cadres spécifiques pour laisser la possibilité de communiquer des renseignements personnels entre organismes, créant des régimes exceptionnels beaucoup plus flexibles que le régime général.

La mise en place de certains programmes, comme ceux qui ont été adoptés dans le cadre du gouvernement électronique, ont également suscité l'adoption de textes spécifiques qui vont permettre la communication de renseignements à caractère exceptionnel, qui n'aident pas vraiment à créer un cadre *ad hoc*, mais qui vont établir une liste d'exceptions à la règle générale.
Nous assistons alors à une accumulation de normes, qui ne font parfois que créer des « sous-régimes » devant cohabiter avec le régime général, ce qui complique davantage les choses pour les citoyens qui désirent savoir à qui et comment sont communiqués réellement leurs renseignements personnels.
Nous observons alors très clairement un phénomène d'accumulation de normes, créant un cadre basé sur la sédimentation, avec tous les problèmes que cela peut comporter.

L'exemple espagnol va illustrer à la perfection cette problématique. Ainsi, le *Tribunal Constitucional* espagnol dans une décision de 2000[651] a déclaré l'inconstitutionnalité d'un alinéa de l'article 21.1 de la *Ley de Protección de Datos de Carácter Personal*[652], encadrant la communication de renseignements personnels au sein des administrations publiques. Cette disposition empêche la communication de renseignements personnels entre organismes appartenant à

[651] *Sentencia 29/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de insconstitucionalidad respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*
[652] *Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal*, BOE-A-1999-23750.

l'administration publique si c'est pour l'exercice de fonctions « différentes » ou pour des fonctions portant sur des matières « différentes » à celles ayant motivé la collecte des renseignements en question.

L'alinéa déclaré inconstitutionnel permettait également la communication entre administrations si le document de création du fichier de renseignements personnels ou si une disposition contenue dans un texte pouvant ne pas être une loi permettaient une telle communication. On pouvait alors imaginer que des ordres ministériels ou des décisions administratives émanant d'une multitude d'organismes puissent permettre de tels transferts.
Le *Tribunal Constitucional* a déterminé que cette disposition allait permettre la communication de renseignements personnels pour des finalités différentes de celles ayant justifié leur collecte, sans le consentement de la personne concernée, sans que celle-ci ne soit informée d'un tel transfert et dans les cas prévus dans des textes pouvant ne pas revêtir la forme d'une loi.

Pour les magistrats espagnols, cet alinéa permettant à un texte à caractère purement réglementaire ou administratif d'autoriser des communications entre administrations est contraire à la protection constitutionnelle accordée en Espagne à la protection des renseignements personnels au paragraphe 18(4) de la Constitution[653].
Ainsi, la rédaction actuelle de l'article 21 de la loi espagnole en la matière va permettre uniquement que les exceptions au régime général de communication des renseignements personnels au sein des administrations fassent l'objet d'une exception si le cas est prévu par l'acte de création du fichier ou par une autre loi occupant la même place dans la hiérarchie des normes dans le système espagnol.

Nous constatons que l'objectif a été de limiter les exceptions au régime général de communication des renseignements personnels et garantir la transparence des

[653] *Constitución Española de 1978*, BOE-A-1978-31229.

échanges, permettant aux titulaires des renseignements personnels d'avoir connaissance de ces communications.

M. Fernández Salmerón[654] souligne qu'aujourd'hui il est possible, par le biais d'une loi, de contourner les cas de communication établis par l'article 21 de la *Ley de Protección de Datos Personales*. Il évoque l'article 92 de la *Ley General Tributaria*[655], encadrant le régime fiscal espagnol, comme un cas paradigmatique de ces exceptions à la règle générale. En effet, cet article, préconisant le « caractère réservé des renseignements à nature fiscale » et imposant la règle générale de la non-communication de ces renseignements, apporte également une liste de 11 cas où la communication est permise entre les différents organismes. Cette tendance, qui se manifeste spécifiquement dans le contexte de la fiscalité, est également observable dans d'autres législations nationales et pas seulement dans le cas espagnol.

Nous constatons alors que les cas exceptionnels finissent par détourner la règle générale quant à la communication de renseignements personnels entre organismes du secteur public. Toutefois, si nous étudions l'article 11 de la *Ley de Protección de Datos Personales*, qui établit le régime général sur la communication de renseignements personnels pour tous les secteurs, nous observons également que les exceptions sont légion.

Ainsi, le paragraphe 11(1) conditionne les transferts de renseignements à un tiers au respect des finalités, puisque la communication doit être motivée par l'accomplissement des fins en rapport direct avec les fonctions légitimes des deux organismes en question, dans les cas où la personne concernée aurait donné son consentement.

Le paragraphe 11(2) de la *Ley de Protección de Datos Personales* établit une liste de six cas où le consentement de la personne concernée ne sera pas nécessaire à la

---

[654] Manuel FERNÁNDEZ SALMERÓN, *La cesión de datos personales en las Administraciones Públicas. Distinción de figuras afines*, Texte de l'allocution dans le cadre de la conférence organisée à l'*Agencia Catalana de Protección de datos*, Barcelona, 25 mai de 2004.

[655] *Ley Orgánica 58/2003, de 17 de diciembre, General Tributaria*, BOE-A-2003-23186.

communication de renseignements personnels. À nouveau, nous constatons dans le droit espagnol que la règle générale basée sur le respect de certaines conditions pour procéder à la communication d'informations se voit vidée de son contenu par une telle liste d'exceptions.

L'exemple du paragraphe 8(2) de la LPRP, présent dans la loi encadrant la protection des renseignements personnels dans le secteur public canadien, témoigne également de l'existence de longues listes d'exceptions permettant le transferts de renseignements personnels.

Pour certains auteurs[656], la lecture de ces cas exceptionnels provoque pour le moins une certaine « perplexité », puisque la protection des renseignements personnels se voit remise en cause tant par la longueur de la liste d'exceptions que par le caractère très général de chacune d'entre elles.

### 2- Éléments pouvant aider à créer un cadre actualisé pour la communication et l'utilisation des renseignements personnels : la problématique du *secondary use*

Nous considérons que suivant notre objectif d'identifier quelques mécanismes pouvant encadrer la protection des renseignements personnels dans les structures en réseau, nous pouvons mettre l'accent sur certaines questions.

Pensons alors au réseau du « cybergouvernement » et aux dangers ou risques que nous pouvons identifier en matière de protection de la vie privée afin d'identifier des mécanismes capables de les « neutraliser » et d'accorder une protection adéquate aux renseignements personnels.

En effet, les « exigences » d'une véritable mise en place d'un cybergouvernement peuvent mettre fin aux silos de renseignements et, par conséquent, en finir avec la protection d'origine « structurelle » qui était accordée aux informations à caractère personnel. Voici l'idée du CPVP[657] à ce sujet :

---

[656] Jesús Alberto MESSÍA DE LA CERDA BALLESTEROS, *La cesión o comunicación de datos de carácter personal*, Madrid, Civitas Ediciones, 2004, p. 109.

[657] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 470, p. 23.

> « Les silos de données sont peut-être contraires au concept de gouvernement en ligne ou cybergouvernement ; il ne fait aucun doute qu'ils sont "moins efficients". Ils dupliquent les renseignements, et on ne peut pas se déplacer de l'un à l'autre. »[658]

Nous avons pu identifier les problèmes potentiels pouvant tirer leur origine de la structure même du réseau et étant à l'origine de la perte de la confidentialité des renseignements personnels.

Pour certains auteurs, dans le contexte de la protection des renseignements personnels, nous pouvons identifier les notions de « risque » et de « dommage ». Ainsi, le risque est présenté comme un événement dont l'occurrence n'est pas certaine mais entraîne pour la personne fichée un dommage[659].
De plus, nous identifions les « facteurs de risques » comme étant « tous les éléments propres à un traitement ou une catégorie de traitements qui sont susceptibles d'avoir une influence sur l'occurrence du risque, soit qu'ils l'augmentent, soit qu'ils la diminuent »[660].

Y. Poullet présente comme un des risques majeurs dans le contexte de la protection de la vie privée la réutilisation des données par d'autres personnes ou pour d'autres finalités[661]. Ainsi, la réutilisation des données constitue un risque si elle est effectuée à des fins différentes de celles qui étaient annoncées initialement ou si elle est le fait de personnes non autorisées initialement, circonstances pouvant toutes deux se cumuler.

---

[658] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE, *Rapport annuel au Parlement 2004-2005 sur la Loi sur la protection des renseignements personnels*, 2005, p. 23.
[659] Yves POULLET, « Réflexions introductives à propos du binôme Droit et sécurité », dans Joël HUBIN (dir.), *Sécurité informatique, entre technique et droit*, Cahiers du C.R.I.D., n° 14, Bruxelles, Story-Scientia, 1998, 185, p. 197.
Cet auteur établit l'existence de trois types de dommage : matériel, immatériel et celui pouvant concerner la sécurité physique des personnes.
[660] Y. POULLET, préc., note 659, p. 198.
[661] *Id.*
Les autres risques encourus peuvent se synthétiser également comme étant la perte de contrôle sur les données, la non-conformité des données et leur inexactitude.

Il faut noter que, comme cet auteur l'a noté, même s'il n'y a pas de détournement de finalité, « la simple utilisation par un tiers non autorisé, pour une finalité éventuellement identique peut constituer un dommage dans certains cas »[662].
Bien sûr, la réutilisation des données présente des risques importants lorsque des facteurs liés aux finalités des données s'ajoutent à cette problématique. Ainsi, pour Y. Poullet la « multiplication des finalités et l'hétérogénéité des finalités poursuivies par la constitution d'une banque de données unique exigeront, en raison des risques plus grands engendrés, des normes de sécurité plus importantes »[663].

D.J. Solove parle du concept de « *secondary use* », qui est l'équivalent de la notion de réutilisation des données quand cette réutilisation est destinée à des fins différentes à celles qui étaient annoncées initialement, et qu'il définit comme il suit :

> « *"Secondary use" is the use of data for purposes unrelated to the purposes for which the data was initially collected without a person's consent. There are certainly many desirable instances of secondary use. Information might be used to stop a crime or to save her life. The variety of possible secondary uses of data is virtually infinite, and they range from benign to malignant.* »[664]

Cet auteur américain établit un lien entre ce concept de « *secondary use* » et le principe de finalité. Ainsi, selon lui, ce « *purpose specification principle* » est reconnu dans le contenu de plusieurs principes et dans les textes législatifs américains en matière de vie privée[665].
De plus, nous retrouvons aux États-Unis un grand nombre de textes normatifs qui limitent le « *secondary use* », ainsi que sur plan international. Toutefois, D.J. Solove souligne qu'aux États-Unis cette reconnaissance est plus limitée qu'ailleurs :

---

[662] Y. POULLET, préc., note 659, p. 200.
[663] *Id.*, p. 205.
[664] Daniel J. SOLOVE, « A taxonomy of privacy », *University of Pennsylvania Law Review*, Vol. 154, n° 3, Janvier 2006, 477, 519.
[665] D. J. SOLOVE, préc., note 9, p. 130.

> « *Although the United States has many laws with secondary-use-restrictions, its protections are less comprehensive than those of many other countries. The problem of secondary use is recognized inconsistently.* »[666]

Il est en outre important de mettre en exergue le rapport que D.J. Solove établit entre le « *secondary use* » et le « *breach of confidentiality* ». L'auteur précise : « *Secondary use resembles breach of confidentiality, in that there is a betrayal of the person's expectations when giving out information* »[667].

Pour d'autres auteurs, même si les principes de protection des renseignements personnels existent aux États-Unis, ils n'ont pas servi à la construction théorique des lois américaines en matière de vie privée. En effet, pour A.B. Serwin, une des questions à se poser est de savoir pourquoi, si Internet et le commerce électronique sont des technologies qui se développent à niveau mondial, les États-Unis n'ont pas adopté les concepts que la plupart des nations partagent[668].

Pour lui, une des raisons qui peuvent expliquer ce phénomène et plus concrètement la non-adoption par les États-Unis des principes de protection des renseignements personnels, trouve son origine dans les différences en matière de règles culturelles sur le partage de l'information.

En effet, cet auteur explique ce phénomène: « *In a very real sense people are in many ways as desirous of privacy as ever, but they want also to enjoy the benefits of increased information sharing, particularly at a time of increased reliance on computers for information* »[669].

Il s'avère très intéressant de voir que A.B. Serwin fait le lien entre une certaine conception du partage des renseignements personnels et la naissance même des sites de réseautage personnels qui ont pour vocation le partage d'informations à

---

[666] *Id*., p. 132.
[667] D. J. SOLOVE, préc., note 664, p. 520.
[668] Andrew B. SERWIN, « Privacy 3.0-The principle of proportionality », 42 *U. Mich. J.L. Reform* 869 2008-2009, 899.
[669] *Id*.

grande échelle : « (...) *the liberal American view of information sharing may be the reason why social networking web sites originated in the U.S.* »[670].

Nous constatons alors que de plus en plus, et notamment à cause de la capacité à partager les renseignements personnels que les structures en réseau nous offrent, les risques peuvent être identifiés.
En effet, nous parlons de « réutilisation des données », de « *secondary use* » ou de partage des informations quand nous voulons identifier les risques informationnels que nous retrouvons dans les réseaux. De plus, nous constatons que nous retrouvons ces « facteurs de risques » des deux côtés de l'Atlantique, bien que le contenu accordé à cette notion soit fort différent.

Les facteurs de risque s'appliquant au contexte de la protection des renseignements personnels en général et aux structures en réseau en particulier requièrent un cadre pouvant tenir compte des protections nécessaires. Ces risques informationnels doivent pouvoir être minimisés, et cela grâce à des mécanismes adaptés à un modèle structurel en forme de réseau permettant de plus en plus le partage d'informations.
Nous examinerons dans les pages qui suivent quels sont les différents éléments pouvant aider à conformer un cadre plus actualisé et effectif de protection. Nous avons vu que le cadre actuel, basé sur la sédimentation de normes et tirant son origine des catalogues d'exceptions se trouvant dans les lois en la matière, ne permet pas d'appréhender les risques informationnels correctement.
Nous verrons comment certains instruments peuvent être utiles afin d'assurer une protection des réseaux et particulièrement des réseaux du secteur public. Il sera surtout question d'analyser les mécanismes les plus adaptés au phénomène du cybergouvernement, afin de permettre une efficacité des services proposés aux citoyens, tout en protégeant leurs droits.

[670] *Id*.

### 3- Des principes de protection des renseignements personnels toujours pertinents pour encadrer la circulation des informations dans les réseaux

Afin de créer un cadre capable de servir comme instrument de gouvernance de ce nouveau modèle d'administration en réseau, nous allons devoir chercher à appliquer le principe de finalité de façon effective. Cette démarche va nous conduire à des règles adéquates pour encadrer les réseaux en général et le nouveau modèle d'administration en particulier.

Nous considérons que le principe de finalité peut encore nous guider dans l'identification des outils pouvant aider à l'application effective du régime de protection des renseignements personnels. Comme certains experts l'ont souligné dans le contexte actuel en vue d'une réforme du régime européen en la matière, il ne s'agit pas à ce stade de « réinventer » la protection des renseignements personnels, mais de chercher une application plus effective des principes de protection dans la pratique :

> « (...) *this is not the time to reinvent data protection. It has already been invented and developed in a process of decades and all energy should now be put in making its principles more effective in practice.* »[671]

Le Contrôleur européen de la protection des données souligne l'idée de renforcement et d'application effective des principes de protection des renseignements personnels au moment où l'on cherche à reformer ou réviser le cadre juridique européen pour la protection des données personnelles. Cette idée est défendue face à ceux qui préconisent la « réinvention » du droit relatif à la protection des données personnelles, plus de quinze ans après l'adoption de la Directive 95/46/CE.

---

[671] CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, « New European rules on data protection », Conférence pronnoncée par Peter HUSTINX au *Joint High Level Meeting on Data Protection Day, Organised by the European Commission and the Council of Europe*, Bruxelles, le 28 janvier 2011 (nous soulignons).

La Commission européenne insiste sur le fait que le double objectif de la Directive 95/46/CE, la protection des droits et libertés des personnes et la libre circulation des données personnelles, est toujours d'actualité. De plus, la Commission affirme que les principes de protection consacrés dans la Directive 95/46/CE restent pertinents et sont toujours valables, et doivent dans tous les cas préserver leur neutralité technologique[672].

Nous assistons depuis quelques années à une « mobilisation » qui tend à renforcer l'idée de réformer le cadre juridique de protection des données personnelles au niveau européen. Ainsi, la Commission européenne, dans une Communication de novembre 2010 suite au lancement d'un examen du cadre juridique actuel et d'une consultation publique, a voulu présenter les résultats de cette consultation et les points les plus importants d'une éventuelle modification de la législation en vigueur[673].
Il nous semble très important, dans le cadre de nos travaux, de constater que nos idées sur la nécessité de trouver un cadre plus adéquat au contexte actuel sont également représentées tant au niveau européen comme au niveau canadien, où une reforme de la LPRP est demandée depuis plusieurs années.

Dans le contexte européen, comme nous avons pu le voir dans les lignes précédentes, l'idée est très claire. Si bien la nécessité de clarifier et de préciser l'application des principes de protection des données personnelles aux nouvelles technologies se confirme[674], la Commission et le Contrôleur européen de la protection des données partagent l'avis que les principes généraux de vie privée et de protection des données restent valides.

---

[672] COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS, *Une approche globale de la protection des données à caractère personnel dans l'Union européenne*, Bruxelles, le 4 novembre 2010.
[673] *Id.*
[674] *Id.*, p. 3.

Suite à l'adoption par la Commission de cette Communication en 2010, le Contrôleur européen de la protection des données publie en janvier 2011 un Avis[675] sur ladite Communication. Le Contrôleur réaffirme la validité des principes de protection : « *The EDPS shares the view of the Commission that a strong system of data protection will still be needed in the future, based on the notion that existing general principles of data protection are still valid in a society which undergoes fundamental changes due to rapid technological developments and globalisation* »[676].

En effet, les importants progrès technologiques et la globalisation sont des facteurs majeurs dans le contexte actuel et la révision du cadre actuel européen en matière de protection des renseignements personnels va devoir tenir compte de ces circonstances.
Pour ce qui nous interesse, nous constatons alors que l'implantation des structures en réseau permettant la circulation des renseignements personnels est vraiment liée à ces phénomènes. De plus, dans le contexte de l'administration électronique ou du cybergouvernement, nous identifions certains phénomènes technologiques présentant des nouveaux défis pour le cadre juridique actuel.

**4- Des nouveaux phénomènes qui demandent d'une protection actualisée**

Pensons par exemple à Internet et à « l'informatique en nuage » ou *cloud computing*, qui va rendre possible la délocalisation du traitement d'une énorme quantité de données à l'échelle mondiale[677]. Certains pensent que le *cloud computing* peut présenter d'importants défis pour ce qui est de l'application des

[675] CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament. The Council, the Economic and Social Committee and the Committee of the Regions – « A comprehensive approach on personal data protection in the European Union »*, 14 janvier 2011.
[676] *Id.*, p. 4 (nous soulignons).
[677] Voir à ce sujet : *Id.*, p. 5.

principes de protection des renseignements personnels[678], notamment par rapport au principe de transparence, de responsabilité et de sécurité.

Certains auteurs décrivent le fonctionnement d'une telle technologie :

> « Les données sont réparties sur un nuage de machines, les centaines de miliers d'ordinateurs-serveurs dont disposent les géants du Web. Les informations étant enregistréees en plusieurs copies dans le nuage, il est possible de répartir les calculs afin d'éviter les congestions informatiques. »[679]

La Commission européenne mentionne également cette technologie afin de démontrer le besoin de réexaminer le cadre juridique actuel, et souligne par rapport au *cloud computing* :

> « L' *informatique en nuage* – c'est-à-dire l'informatique fondée sur l'Internet dans le cadre de laquelle des logiciels, des ressources et des informations partagées se trouvent sur des serveurs lointains (*dans les nuages*) – pourrait également lancer les défis dans le domaine de la protection des données car elle peut signifier, pour le particulier, une perte de contrôle sur les informations potentiellement sensibles qui le concernent, lorsqu'il stocke ses données à l'aide de programmes hébergés sur l'ordinateur de quelqu'un d'autre. »[680]

Nous pouvons penser à l'utilisation d'une telle technologie dans le contexte des réseaux du gouvernement et il est facile d'imaginer les enjeux que l'utilisation d'une telle option va présenter en matière de protection de la vie privée.

Pensons également aux réseaux sociaux et aux risques associés à un tel phénomène dans le cadre des communications entre les administrations et les citoyen dans le contexte du gouvernement en ligne. D. Keats Citron présente un aperçu des

---

[678] Yves POULLET, « Cloud Computing and Privacy Issues – first reflections », Présentation lors du Séminaire « Privacy and Security », organisé par *l'Agencia Española de protección de datos* dans le cadre du Projet « Vie Privée et Sécurité », Madrid, 8 juin 2010.

[679] Hervé LE CROSNIER, « À l'ère de l' informatique en nuages », *Le Monde diplomatique, Manière de voir, Internet, révolution culturelle*, no. 109, 109, février-mars 2010, 74.

[680] COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS, préc., note 672, p. 2.

problèmes découlant des « *Government 2.0 sites* »[681] et présente sa vision du « *One way mirror* » en vue de préserver le droit à la protection de la vie privée dans ce contexte :

> « *(...) government should view Government 2.0 sites as one-way mirrors, where individuals can see government's activities and engage in policy discussion, but where government cannot use, collect or distribute individuals'social media information. This would advance the goal of open government. Strong privacy rules enhance deliberative democracy by encouraging participation and by discouraging self-censorship.* »[682]

Nous pouvons alors réfléchir aux dangers pouvant découler de l'utilisation des renseignements des citoyens provenant des sites sociaux à d'autres fins que ceux qui auraient justifié leur collecte. Ainsi, au lieu de servir aux seules fins de « *policymaking purposes* », on peut imaginer un partage d'informations de la part du gouvernement entre organismes différents et pour des finalités très variées. Voici comment on peut décrire un tel danger : « *Rather than using a person's social-media data for policy-making purposes, executive departments and agencies could share it with law-enforcement, immigration and tax authorities* »[683].

En effet, la mise en place de toutes ces nouvelles technologies et l'utilisation d'Internet dans le contexte des applications d'un État en réseau ne font que renforcer l'idée du besoin d'un cadre permettant de relever efficacement de tels défis. De plus, si nous pensons à l'image d'une administration électronique, qui se caractérise par la mise en place de technologies basées sur le Web 2.0 et qui utilise des solutions offertes par le *cloud computing*, l'image de réseau est plus réelle que jamais !

---

[681] Danielle KEATS CITRON, «Fulfilling Government 2.0's Promise with Robust Privacy Protections», 78 *George Washington Law Review*, A-101 (2010).
Ce texte parle des possibilités offertes par cette modalité de gouvernement : « *Government 2.0 permits a «two way interaction between government and its citizens » through online comments, live chats, and message threads ».*
[682] *Id.*,p. A-106.
[683] *Id.*, p. A-110.

Il est intéressant de constater que nous retrouvons ce besoin de « révision » du cadre actuel en matière de protection des renseignements personnels dans le secteur public au Canada, mais également dans le contexte européen.

De plus, les voix qui réclament des changements et qui demandent l'adoption de mesures afin de rendre le système de protection plus efficace affirment également la pertinence et l'actualité des principes directeurs de protection des renseignements personnels. Nous avons pu constater que la Commission européenne et le bureau du Contrôleur européen partagent cet avis et nous observons qu'au Canada les voix qui réclament la réforme de la LPRP veulent que ce texte se rapproche de la LPRPDE, texte applicable au secteur privé et articulé autour des principes du code type de la CSA.

Dans le cadre de nos travaux, nous avons voulu démontrer le besoin actuel d'identifier les mécanismes de protection de la vie privée les plus adaptés aux nouvelles formes de circulation des données, notamment dans les environnements en réseau. Nos travaux ont également eu pour objet d'analyser le principe de finalité et de réaffirmer le rôle que ce principe a joué, joue et doit jouer dans l'avenir pour encadrer la protection des renseignements personnels.
Nous allons présenter dans les pages qui suivent quelques pistes pouvant nous aider à identifier les mécanismes capables de servir dans le futur à bâtir un cadre efficace et adapté aux nouveaux phénomènes techniques et de tenir compte des effets de la globalisation.

## 5- Les ententes bilatérales comme outil encadrant le partage de renseignements personnels : un instrument de transition ?

Au Canada, nous observons également depuis des années une augmentation du nombre d'ententes entre les organismes qui établissent un accord de partage et de communication de renseignements personnels. Ces accords bilatéraux sont un instrument qui peut vraiment aider à baliser les conditions de communication des

renseignements, si elles respectent des conditions minimales capables de créer un cadre de protection pour les renseignements personnels en question.
D.H. Flaherty présente les ententes de partage comme étant une composante aidant à couvrir la nécessité d'une gestion des renseignements personnels pour les services du gouvernement électronique.

Pour lui, « l'utilisation et le partage pangouvernemental de renseignements personnels présentent un intérêt particulier lorsqu'ils ont trait à la prestation de services »[684]. Pour cet expert, il est possible de contrôler un tel partage d'informations en amenant les entités gouvernementales à signer entre elles des ententes de partage de données qui sont « essentiellement des contrats exécutoires »[685]. Pour cet expert, les ententes de partage des données peuvent aider à créer un cadre de protection, puisqu'elles comportent des règles et des responsabilités et assurent la transparence aux fins de la protection de la vie privée[686].

Bien sûr, nous partageons cet avis, mais nous observons également que le nombre très important d'ententes bilatérales établissant le régime de partage entre l'ensemble des organismes publics pour les innombrables programmes qui existent aujourd'hui peut poser problème, notamment si nous sommes à la recherche « d'une vraie transparence » de ces échanges.
De plus, la mise en place des services du gouvernement électronique au Canada, ainsi que dans la plupart des pays développés, n'a fait que multiplier la signature de ces ententes, en vue de créer des bases de données globales ou de fusionner des bases de données existantes qui renferment un grand volume de renseignements personnels.
Penser à un gouvernement électronique qui fonctionne grâce à des contrats entre organismes peut nous faire croire que cet instrument est un élément ou un indice du caractère réseautique de ces échanges. Toutefois, nous considérons que cette image

[684] D. H. FLAHERTY, préc., note 262, p. 19.
[685] *Id.*
[686] *Id.*, p. 20.

peut continuer à nous faire penser plutôt à deux silos communicants, même si nous considérons que l'entente constitue un instrument capable d'encadrer très convenablement ces échanges afin de protéger les renseignements personnels.
Vu le nombre croissant d'ententes entre organismes, parfois à l'étranger, il va devenir très difficile pour le citoyen de repérer si ses renseignements personnels sont concernés par chacune de ces ententes. Il semble que si nous voulons arriver à garantir un niveau acceptable de transparence dans les modalités des échanges se produisant dans les réseaux, cet instrument n'est probablement pas le plus adéquat.

Ainsi, tout en affirmant que cet instrument présente des avantages importants afin de protéger les renseignements personnels, nous pensons qu'il s'agit plutôt d'un « procédé de transition », qui n'est pas vraiment réseautique et qui garde encore des attributs pouvant nous faire penser au modèle de l'État en silo.
Aujourd'hui, cet instrument peut effectivement contribuer à ce que les échanges de données se produisent à l'aide d'un instrument capable d'encadrer la protection des renseignements faisant l'objet d'une telle entente.

Le domaine du partage des données pour des questions liées á la sécurité nationale et à la lutte antiterroriste a considérablement fait augmenter la signature de ces ententes. Il est d'ailleurs préoccupant de constater l'augmentation du nombre d'ententes signées entre des organismes du secteur public du Canada et des États-Unis depuis 2001, permettant ainsi un transfert massif d'informations.

En effet, la situation se complique notamment parce que les transferts de renseignements personnels peuvent se faire entre des gouvernements au niveau national mais aussi en traversant les frontières nationales. Le cas est particulièrement grave au Canada, pays qui ne dispose pas de règles limitant ces transferts vers des pays tiers. Il faut souligner que dans le cas de l'Union Européenne, des règles contenues dans la Directive 95/46/CE limitent les transferts de données uniquement aux pays ayant un niveau de protection adéquat.

Lors de la vérification par le CPVPC des pratiques de gestion des renseignements personnels par l'Agence des services frontaliers du Canada[687], il a été constaté que dans le contexte de la signature des ententes avec les organismes des États-Unis, ni cette Agence ni le CPVPC ne connaissaient vraiment l'usage que les Américains allaient faire des renseignements transmis[688].

De plus, cette Agence n'est pas en mesure d'affirmer que ces échanges de données avec les États-Unis respectent les conditions minimales que les lois canadiennes en la matière imposent :

> « L'ASFC ne peut, avec un degré raisonnable de certitude, faire rapport de la mesure dans laquelle ont lieu les échanges de renseignements personnels avec les États-Unis, le volume ou la fréquence de ces échanges. En outre, l'ASFC ne peut être certaine que toutes ses activités d'échange de renseignements sont autorisées en vertu de l'article 107 de la Loi sur les douanes et de l'article 8 de la Loi sur la protection des renseignements personnels. »[689]

Bien sûr, nous considérons que la signature des ententes de partage avec des organismes étrangers doit toujours être conditionnée de manière à connaître à la perfection les finalités auxquelles les renseignements serviront après ce transfert. Le respect des dispositions législatives canadiennes pouvant s'appliquer à de tels transferts nous semble également important afin de garantir la légalité de ces transferts.

Les ententes sont normalement utilisées dans le cadre des échanges avec des organismes que l'alinéa 8(2)f) de la LPRPDE encadre[690]. Il faut dire que le CPVPC

---

[687] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport de vérification des pratiques de gestion des renseignements personnels de l'Agence des services transfrontaliers du Canada*, Juin 2006.

[688] D. H. FLAHERTY, préc., note 262, p. 21.

[689] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 687, p. 23.

[690] Cet alinéa encadre les cas de « communication aux termes d'accords ou d'ententes conclus d'une part entre le gouvernement du Canada ou l'un de ses organismes et, d'autre part, le gouvernement d'une province ou d'un État étranger, une organisation internationale d'États ou de gouvernements, le conseil de la première nation de Westbank, le conseil de la première nation participante — au sens du paragraphe 2(1) de la *Loi sur la compétence des premières nations en matière d'éducation*

établit une liste de critères élaborés à partir de diverses sources, et devant être inclus dans les accords et ententes d'échange d'informations personnelles[691].

Si nous analysons les questions de partage d'informations entre l'Agence de santé publique du Canada et les ordres du Gouvernement, nous identifions une problématique, qui trouve son origine dans certaines lacunes en matière d'accords pour le partage de données, devant fournir un cadre suffisant dans les cas d'urgence en matière de santé publique, tout en protégeant les renseignements personnels.

Ainsi, la Vérificatrice générale du Canada a pu constater, en 2008, que l'Agence de santé publique du Canada, afin d'officialiser la coopération avec les provinces et territoires, a élaboré un « accord intergouvernemental » sur le partage de données[692].

De plus, l'Agence de santé publique du Canada collabore depuis des années avec les provinces et territoires afin de mettre en place des « ententes » relatives au partage des données[693].

En effet, il est important de prévoir que, lors d'une urgence en matière de santé publique et tout en respectant la LPRP, des « ententes » relatives au partage des données puissent établir les conditions minimales à respecter pour que rien n'empêche la circulation des informations, quand cela s'avère nécessaire, tout en protégeant des renseignements sur la santé, de nature spécialement délicate.

Certains n'hésitent pas à recommander vivement que la LPRP indique clairement les exigences à inclure dans chaque accord de partage de renseignements personnels, ainsi que « les exigences en matière de reddition de comptes et d'établissement de rapports relativement à ces accords »[694].

---

*en Colombie-Britannique* — ou l'un de leurs organismes, en vue de l'application des lois ou pour la tenue d'enquêtes licites ».

[691] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 687, p. 70 à 75.

[692] BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA, *Rapport de mai 2008 sur Rapport de la vérificatrice générale du Canada - Chapitre 5 - La surveillance des maladies infectieuses*, p. 38.

[693] *Id.*, p. 24.

[694] D. H. FLAHERTY, préc., note 262, p. 21.

Nous considérons que des contrôles *a priori* sur le contenu et les conditions de ces ententes s'imposent, afin d'assurer le respect des principes basiques en matière de protection des renseignements personnels. De plus, des examens *a posteriori* complètent le contrôle qui doit encadrer la signature et l'entrée en vigueur de ces ententes de partage, si nous voulons assurer la protection des renseignements personnels transmis à l'intérieur et à l'extérieur des pays. Dans le cas du Canada, il nous semble crucial aujourd'hui d'introduire la nécessité de ces contrôles dans la LPRP ainsi que des règles minimales devant être observées dans la rédaction des ententes.

Le CPVPC[695] s'est penché sur la manière dont les institutions fédérales respectent les exigences en matière de présentation de rapports annuels ministériels au Parlement sur la protection des renseignements personnels. Le Secrétariat du Conseil du Trésor exige, en vertu de l'article 72 de la LPRP, que les ministères et organismes produisent un rapport annuel sur la façon dont ils administrent cette question.

Le CPVPC a pu constater que, dans bien des cas, les rapports ne permettent pas de comprendre ce que font les organismes avec les renseignements personnels qu'ils possèdent ni la façon dont ils gèrent les risques connexes[696].

De plus, le CPVPC a pu constater que, parmi les éléments obligatoires devant figurer dans les rapports, un des éléments les plus souvent absents est celui faisant référence aux types de communication faites en vertu des paragraphes 8(2)a) à 8(2)m) de la LPRP au cours de l'année visée par le rapport. En outre, le rapport concernant toute nouvelle activité de partage des renseignements personnels, et cela « par l'entremise de banques de données à l'interne, ainsi qu'avec d'autres organismes »[697], manque lui aussi.

---

[695] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Vérification des Rapports annuels fédéraux sur la protection des renseignements personnels*, 2009.
[696] *Id*., p. 4.
[697] *Id*., p. 11.

Nous observons que le Secrétariat du Conseil du Trésor impose l'obligation d'inclure, comme une des exigences en matière de production des rapports, « le nombre de nouvelles activités de couplage et de partage de données entreprises, y compris les activités à l'interne entre les différentes unités de l'institution et une brève description de chacune »[698].

Toutefois, comme le CPVPC l'a constaté, ces obligations ne sont nullement respectées et les organismes n'incluent pas habituellement ces informations, qui à notre avis sont de la plus grande importance. Si ces informations étaient contenues dans les rapports produits par les organismes publics, nous serions en mesure de connaître les risques pouvant être identifiés au sein du secteur public. La transparence nous semble être le seul outil capable de garantir le respect du paragraphe 8(2) de la LPRP.

Nous identifions, dans tous les domaines, une tendance à vouloir régler la question des échanges de données entre organismes, par la signature d'ententes *ad hoc*. Cet instrument nous semble d'une grande utilité et est probablement le seul capable, à l'heure actuelle, d'encadrer convenablement le partage entre les autorités au sein du secteur public.

Ces ententes, pouvant être signées entre organismes appartenant au niveau national ou fédéral, mais également avec des organismes appartenant à l'administration des provinces ou des municipalités, sont de plus en plus nombreuses. Même si ces ententes font normalement l'objet de diffusion, les différentes sources d'information et d'accès au contenu de telles ententes peut compliquer la tâche des citoyens qui cherchent à connaître la diffusion qui est faite de leurs renseignements, dans quel but et dans quelles conditions.
À cause du grand nombre d'ententes bilatérales, qui ne sont pas toujours faciles à repérer pour le citoyen, on se trouve clairement dans un cas de manque de transparence.

---

[698] *Id.*, p. 19.

De plus, le citoyen ne participe nullement au processus qui donne lieu à la décision sur le contenu des ententes, et cela parce que le choix des données qui seront partagées, des organismes entre lesquels ces échanges auront lieu et les finalités en vertu desquelles elles seront traitées, n'est connu des personnes concernées qu'après la signature d'un tel instrument.

Certains ont identifié les risques d'entrave à la vie privée que posent les ententes d'échange de renseignements personnels : fondement juridique inexistant ou douteux, profilage ou appariement de données, surveillance des opérations, identification des personnes, mesures de sécurité insuffisantes et utilisation ou divulgation d'informations à des fins accessoires[699].
Nous observons alors que, au Canada, l'Institut des services axés sur les citoyens a identifié comme un des risques majeurs dérivés de la signature d'une entente l'utilisation des renseignements personnels à des fins pouvant dépasser les finalités ayant motivé leur collecte, ce qui prouve à nouveau l'existence de problèmes liés au principe de finalité pouvant tirer leur origine de l'échange de données entre organismes du secteur public.

Cet institut a produit un document présentant les lignes directrices sur les pratiques exemplaires en matière d'ententes d'échanges de renseignements personnels où il établit une liste de catégories d'ententes qui aident les organismes à identifier quelle catégorie peut convenir au mieux aux différents échanges d'information. Ainsi, nous identifions des transmissions répétées, une transmission unique, une transmission unidirectionnelle et une transmission bidirectionnelle.
En effet, pour cet institut, une des fonctions des ententes est de « préciser le fondement juridique qui autorise une partie à recueillir et à divulguer de l'information, les motifs auxquels elle doit servir, l'information exacte requise et les mesures de sécurité particulières dont elle sera l'objet »[700]. De plus, ces lignes

[699] INSTITUT DES SERVICES AXÉS SUR LES CITOYENS, *Ententes d'échange de renseignements personnels, Lignes directrices sur les pratiques exemplaires*, p. 36, en ligne : http://www.iccs- isac.org/fr/practice/privacy.html (consulté le 15 mai 2011)
[700] *Id*., p. 9.

directrices soulignent que, en règle générale, les ententes doivent être bilatérales, visant à la fois la partie qui divulgue et celle qui reçoit l'information et prévient des dangers d'une « entente multilatérale » qui engendre le risque de traiter les questions importantes susmentionnées en des termes trop vagues ou généraux[701].

Les lignes directrices de l'Institut des services axés sur les citoyens énumèrent six pratiques exemplaires importantes constituant les « étapes du processus décisionnel, allant du recensement des besoins à la surveillance des ententes »[702].

Les trois premières pratiques doivent s'appliquer avant la conclusion de l'entente et les pratiques 4 à 6 s'appliquent après que la décision de conclure une entente a été adoptée. La première des pratiques est le « recensement des besoins et des facteurs de risque », imposant deux conditions obligatoires à remplir : posséder le pouvoir légal nécessaire et le besoin clair et justifiable de communiquer les informations en question[703].

La deuxième pratique est un « Examen de stratégies de substitution », afin de trouver des solutions de rechange possibles, telles que « fournir un résumé de l'information et ne pas révéler l'identité des personnes concernées ; rendre les données anonymes ; fournir des données agrégées, par exemple une fourchette d'âges plutôt que des âges particuliers »[704].

Par la suite, il faut procéder à une « Évaluation des risques », qui comprendra notamment une Évaluation des facteurs relatifs à la vie privée, ÉFVP, un des outils recommandés par ces lignes directrices afin d'identifier les risques d'entrave à la vie privée.

---

[701] *Id.*
[702] *Id.*, p. 3.
[703] *Id.*, p. 5.
[704] *Id.*, p. 6.

La quatrième des pratiques comporte la « Documentation de la décision », qui consiste à « consigner la décision d'aller de l'avant, afin de la justifier et de décrire à grands traits un plan d'atténuation des risques »[705].
La cinquième de ces pratiques est relative à l'établissement de l'entente devant comporter toute une série d'éléments clés que les lignes directrices établissent dans une liste[706] et devant observer des précautions particulières, telles que la nomination d'un conseil de surveillance composé des membres de l'organisme qui connaissent les questions de protection de la vie privée.
Finalement, la dernière des pratiques est relative au contrôle de l'efficacité de l'entente et comporte un suivi et une autoévaluation visant à examiner et vérifier toutes les questions relatives à une telle entente.

Ce document est, à notre avis, une guide qui peut aider considérablement les organismes lorsqu'il leur est nécessaire de communiquer des renseignements personnels afin « d'apprécier l'exactitude d'information sur des particuliers ou d'évaluer l'admissibilité à un programme ou un service »[707], dans le cadre des services offerts aux citoyens.
La nature de ces lignes directrices n'ayant pas de force contraignante, elle n'oblige nullement les organismes du secteur public canadien à respecter ces indications devant accompagner la signature d'une entente d'échange de renseignements personnels.

Au Canada, au niveau fédéral, nous retrouvons une situation qui démontre que ces ententes peuvent être à l'origine de situations problématiques. Ainsi, comme

[705] *Id.*, p. 6.
[706] *Id.*, p. 7.
Cette liste comporte ces éléments clés : « l'identité, les rôles et les responsabilités des parties ; l'information divulguée et recueillie et le motif dans chaque cas; la fréquence des échanges et la durée de l'information échangée ; le fondement juridique de la divulgation et de la collecte de l'information ; les méthodes de transmission et de stockage de l'information et les mesures de sécurité prises ; la marche à suivre en cas d'entrave à la vie privée ou à la sécurité; les restrictions à la collecte, à l'utilisation, à la divulgation et à la conservation d'information; des mesures visant à garantir l'exactitude de l'information ; l'indemnisation prévue ; la surveillance de la conformité ».
[707] *Id.*, p. 14.

certains l'ont souligné[708], le CPVPC peut donner des conseils, mais les institutions fédérales ne sont nullement obligées de les suivre.

Nous pouvons donc imaginer que le CPVPC se trouve dans une position compliquée pour empêcher la signature de certaines ententes entres organismes appartenant au secteur public fédéral ou, pour le moins, pour modifier certains de ses points ou conditions. Nous constatons que la LPRP n'impose aucune exigence à inclure dans les ententes de partage entre organismes et n'a aucune prétention en matière de reddition de comptes ou, moins encore, sur les contrôles du respect de ces ententes lors des échanges d'informations entre les organismes publics.

Certaines dispositions de la LPRP, notamment celles qui autorisent la communication et l'usage des renseignements personnels par les institutions fédérales et sans le consentement des personnes concernées, sont « trop » flexibles et laissent la porte ouverte à de potentiels abus. De plus, tant que le CPVPC n'aura pas le pouvoir de rendre des ordonnances, nous ne pouvons pas affirmer que tous les secteurs du gouvernement vont leur prêter attention. D.H. Flaherty illustre, à notre avis, cette problématique à la perfection :

> « Aujourd'hui, il est extrêmement facile pour les ministères et les organismes fédéraux de ne voir en la commissaire à la protection de la vie privée qu'une personne seulement capable de prodiguer des conseils que nul n'est obligé de prendre en considération. »[709]

Voici quelques pistes afin de comprendre le fonctionnement du cadre basé sur les exceptions à la règle générale et sur la signature des ententes bilatérales afin de partager des informations entre organismes. Ce cadre ne semble pas être le plus transparent ni le plus cohérent des régimes de gouvernance pour les réseaux. Dans le cas canadien, le manque d'un réel pouvoir du CPVPC pour contrôler les exigences contenues dans les ententes de partage n'aide pas à considérer cet instrument comme le plus adapté aux besoins du gouvernement électronique.

---

[708] D. H. FLAHERTY, préc., note 262, p. 17.
[709] *Id*., p. 33.

Ces ententes et ce régime de « sédimentation » de normes et règles de natures très variées – les unes créées pour encadrer un modèle d'administration en réseau, les autres adoptées pour gouverner des structures en silo –, ne présentent pas les conditions nécessaires pour encadrer un « vrai réseau » où les informations circuleraient de forme contrôlée.

Il nous semble que les ententes répondent beaucoup plus à la logique du silo qui se connecte à un autre silo, comme le CPVPC l'a affirmé : « les silos de données sont l'antithèse des concepts de cybergouvernement ou de "Gouvernement en direct" »[710].

De plus, le besoin du recours automatique aux listes d'exceptions à la règle générale nous semble être un symptôme à ne pas négliger. En effet, la longue liste des exceptions, chacune plus « ouverte » que l'autre, nous laisse deviner que les mécanismes pour contourner les bases de la législation en matière de protection des renseignements personnels ont réellement été mis en place !

Nous considérons qu'aujourd'hui la communication de renseignements personnels entre organismes du secteur public est généralement basée sur le contournement de la règle générale posant les limites à de telles communications.

Le philosophe italien G. Agamben a su clairement identifier comment, dans le contexte actuel, suite aux attaques terroristes de 2001, les mesures adoptées en matière de sécurité ont provoqué l'avènement de « l'état d'exception comme paradigme de gouvernement »[711]. Bien sûr, cet auteur parle d'un contexte beaucoup plus vaste que celui qui fait l'objet de notre étude, mais ses propos sont très facilement transposables à tout autre scénario actuel.

En effet, en faisant référence aux mesures adoptées afin d'assurer la sécurité nationale cet auteur identifie un phénomène pouvant avoir comme résultat la limitation permanente de certains droits. Ainsi, cet auteur parle du fait que la « création volontaire d'un état d'urgence permanent (même s'il n'est pas déclaré au

[710] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 324, p. 6.

[711] Giorgio AGAMBEN, *État d'exception, Homo Sacer*, Paris, Éditions du Seuil, 2003, p. 10.

sens technique) est devenue l'une des pratiques essentielles des États contemporains, y compris de ceux que l'on appelle démocratiques »[712].

À notre avis, c'est effectivement dans le contexte de la lutte antiterroriste que nous pouvons observer que l'application de mesures exceptionnelles, telles que le partage d'informations à grande échelle et la création de listes de personnes interdites au vol, est devenue une forme de gouvernance plus ou moins acceptée dans nos sociétés. En parlant d'un « passage d'une mesure provisoire et exceptionnelle à une technique de gouvernement »[713], G. Agamben souligne les dangers potentiels de l'application des mesures d'exception pouvant limiter les droits des personnes de façon permanente.

Dans le contexte de nos travaux, nous considérons que baser le cadre de circulation des renseignements personnels dans le réseau gouvernemental sur des régimes exceptionnels ou sur la signature de milliers d'ententes entre organismes n'est pas la solution la plus adaptée au mode de circulation « réseautique ».
Si nous acceptons que le modèle de circulation en réseau présente des risques et a des limites pouvant avoir un impact majeur sur la protection des renseignements personnels, il vaut mieux prévoir des mécanismes de protection plus adaptés à cette structure.
Le fait d'être régi par un régime de circulation des renseignements personnels conformé par des mécanismes qui se basent sur des exceptions au régime général démontre, à notre avis, une problématique non négligeable. Ces mécanismes qui font exception à la règle générale qui repose sur le principe de finalité ne sont pas les plus adaptés aux structures en réseau dans lesquelles les renseignements personnels circulent aujourd'hui.
Ces ententes bilatérales sont plutôt un instrument qui annonce le fait que l'on avance vers une gouvernance de type réseautique et nous considérons qu'il s'agit

[712] *Id.*, p. 11.
[713] *Id.*, p. 12.

plutôt d’un élément de transition vers ce modèle visant à encadrer convenablement l’État en réseau.

La sécurité juridique des titulaires des renseignements personnels et la transparence nécessaire aux échanges d’informations ne peut pas être assurée par un régime basé sur les exceptions. La gouvernance des structures en réseau permettant la circulation des renseignements personnels nécessite des mécanismes d’adaptation réseautiques qui, s’ils répondent très clairement aux principes de protection des renseignements personnels, contribuent à une application plus effective de ces principes dans ces structures de circulation des informations.

## SECTION 2 Quelques pistes pour l'adoption de mécanismes d'adaptation « réseautique » pour la protection des renseignements personnels

Nous allons identifier dans les pages qui suivent les mécanismes de gouvernance capables de tenir compte des spécificités des environnements en réseau. À notre avis, tous ces mécanismes ont une capacité d'adaptation réseautique, puisqu'ils sont capables de servir à protéger les renseignements personnels dans les circonstances toujours changeantes qui caractérisent les réseaux.

Tous ces mécanismes peuvent être mis en place individuellement ou en combinant leur application, afin de créer un cadre de protection efficace. Il nous semble que ce sont des outils pouvant offrir des solutions de protection pour les structures en réseau du secteur public. Bien sûr, nous en imaginons très bien la mise en œuvre dans le contexte des services offerts dans le cadre d'une administration électronique et plus généralement dans les structures en réseau où les informations ont tendance à circuler de plus en plus.

Cette liste non exhaustive veut être la compilation de quelques solutions de différentes natures que nous jugeons d'une grande utilité dans la recherche d'instruments utiles pour établir un cadre de gouvernance adéquat.

Nous considérons que certains de ces mécanismes aident à respecter les lois de protection des renseignements personnels, s'appuyant très souvent sur le contenu et l'étendue des principes de protection des renseignements personnels et contribuant ainsi à les concrétiser et à leur offrir une application effective.

### 1- Les évaluations des facteurs relatifs à la vie privée ou *Privacy Impact Assessment* face aux risques en matière de protection des renseignements personnels

Nous considérons que les évaluations des facteurs relatifs à la vie privée ou ÉFVP sont des outils vraiment adaptés aux conditions prévalant dans les structures en réseau. Il faut rappeler que les ÉFVP ou *Privacy Impact Assessment* (PIA) ont été

définies comme des « processus d'élaboration des politiques permettant de déterminer, d'évaluer et d'atténuer les risques d'entrave à la vie privée »[714].
Le gouvernement canadien a été « pionnier à l'échelle internationale »[715] en ce qui concerne l'usage des ÉFVP afin d'assurer que la protection de la vie privée a été prise en considération dans le cadre de la mise en place de programmes et d'initiatives impliquant le traitement des renseignements personnels dans le secteur public.

Comme nous avons pu le constater dans les pages précédentes, les ÉFVP servent principalement à repérer d'éventuels risques d'entrave à la vie privée engendrés par les programmes et services des institutions fédérales et sont des instruments vraiment utiles pour réduire ou éliminer ces risques.
Le CPVPC souligne que, lorsque les institutions fédérales présentent des ÉFVP au CPVPC, ces évaluations doivent montrer que l'initiative proposée est vraiment nécessaire et qu'elle est sera sans doute indispensable afin d'atteindre le but envisagé.
De plus, la CPVPC affirme que les ÉFVP « doivent montrer que l'ingérence dans la vie privée est proportionnée aux avantages prévus et qu'il n'y a pas d'autres solutions qui seraient moins envahissantes pour la vie privée »[716].

P. Trudel nous rappelle que la protection des informations faisant partie de la vie privée relève d'une « logique de risques » et que, plus généralement, « la normativité relative à Internet est en grande partie motivée par le souci de réduire, gérer et répartir les risques découlant d'informations sur Internet » [717]. Cet auteur

[714] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 523.
[715] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Nos attentes : Un guide pour la présentation d'évaluations des facteurs relatifs à la vie privée au Commissariat à la protection de la vie privée du Canada*, mars 2011, p. 2.
[716] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La protection de la vie privée à l'ère du gouvernement 2.0*, Commentaires présentés par Jennifer STODDART à l'occasion du Salon des gouvernements innovateurs du Canada 2010 « Les gouvernements hautement performants », le 7 octobre 2010, Ottawa, Ontario.
[717] Pierre TRUDEL, *Normativités en réseau et gestions des risques par les états et les usagers d'Internet*, Analyse réalisé dans le cadre d'un programme de recherche sur les méthodes de régulation des médias dans la nouvelle économie financée en partie par le Groupe TVA en vertu

assure également que le système de régulation a pour objectif de rétablir l'équilibre entre les risques et les précautions.

Certains voient les processus d'ÉFVP comme « un exercice de dilligence raisonnable qui permet aux institutions de déterminer et d'atténuer les risques d'entrave à la vie privée qui pourraient survenir au cours de leurs opérations »[718].
En effet, à notre avis, cet outil constitue un mécanisme capable d'aider à gérer les risques pour les organismes du secteur public notamment dans le cadre des environnements en réseau.
Dans le contexte européen, nous entendons parler plutôt d'« études d'impact » en matière de protection des renseignements personnels, et cela avant la mise en place d'un projet au sein des institutions du gouvernement.
Nous considérons que l'analyse des questions reliées aux risques concernant la circulation des renseignements personnels répond à une logique équivalente à celle qui est appliquée dans le contexte des risques environnementaux. Ainsi, au Canada, pour certains « les évaluations des facteurs relatifs à la vie privée devraient être aussi courantes que les évaluations des incidences environnementales »[719].

Y. Poullet avance l'idée de l'application d'un certain nombre de principes qui viennent du droit de l'environnement au contexte des nouvelles technologies de l'information, puisque celles-ci vont structurer l'espace et les relations se déroulant dans cet espace. Il cite très concrètement « le principe de partage des risques » en raison des risques créés et le « principe de précaution », constituant tous deux des pistes importantes pour l'avenir dans le contexte de la protection des données personnelles[720].

---

d'une contribution versée dans le cadre du programme des avantages tangibles mis en place lors de la transaction par laquelle Québécor Media a acquis le contrôle de TVA.

[718] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Règlement fédéral sur la protection des renseignements personnels en 2010 : le bilan*, Commentaires présentés par Patricia KOSSEIM à l'occasion de la 6e conférence annuelle de FJP sur le droit administratif organisée par Osgoode Law School, le 19 octobre 2010, Toronto, Ontario, en ligne : "http://www.priv.gc.ca/speech/2010/sp-d_20101019_pk_f.cfm" (nous soulignons).

[719] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Commentaires présentés par Chantal BERNIER, préc., note 533.

[720] Y. POULLET, préc., note 15.

Il nous semble que les processus d'ÉFVP répondent d'une certaine façon à cette idée, à cause de leur objectif de gestion du risque, et cela avant la mise en place d'un système ou projet comportant la gestion de renseignements personnels et présentant des dangers pour la vie privée.

Dans le contexte de la sécurité, le CPVPC dans son document « Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle »[721] affirme que l'ÉFVP dans le secteur public est à la vie privée ce que les « évaluations de la menace et des risques » (EMR) sont aux enjeux de sécurité.
Quand nous observons comment se passent les choses dans d'autres domaines, tels que celui de l'environnement ou celui de la sécurité, nous observons que la gestion des risques est réalisée à partir de la mise en place de processus très clairs et homogènes et que l'adoption de projets ou programmes est toujours précédée du déroulement de ces processus d'évaluation.
À notre avis, pour ce qui est des questions de vie privée, ces ÉFVP devraient toujours être obligatoires dans le secteur public avant la mise en place de projets comportant la gestion des renseignements personnels.
Que la loi en la matière oblige à réaliser ces évaluations peut sans doute renforcer l'importance de tels processus. Le CPVPC a proposé que la réforme de la LPRP puisse inclure que le processus d'ÉFVP soit obligatoire en vertu de la loi. Aujourd'hui, l'obligation pour les institutions publiques de procéder à l'application de ces démarches au Canada n'est pas contenue dans la LPRP ni dans aucune loi ou règlement en vigueur, mais dans une directive du Secrétariat du Conseil du Trésor[722]. Il faut se rappeler que le CPVPC a dénoncé dans le passé un manque d'efficacité de la politique sur les ÉFVP et affirme qu'elle serait sans doute plus efficace si elle avait force de loi[723].

---

[721] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 634.
[722] SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Directive sur l'évaluation des facteurs relatifs à la vie privée*, 1er avril 2010, en ligne : http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308 (consulté le 10 juillet 2011).
[723] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information sur les ÉFVP*, 2007, en ligne : http://www.priv.gc.ca/fs-fi/02_05_d_33_f.cfm (consulté le 7 juin 2011).

Dans un autre contexte, celui des États-Unis, nous observons que, à partir de 2002, dans le cadre des projets comportant le traitement de renseignements personnels au sein des organismes du secteur public, il existe une obligation légale de procéder à une PIA ou *Privacy Impact Assessment*. En effet, le *E-Government Act*[724] de 2002 établit dans sa Section 208 l'obligation pour chaque agence du gouvernement de procéder à la réalisation d'une PIA qui, si possible, va devoir faire l'objet d'une publication sur le site web de l'institution en question.

De plus, le *E-Government Act* établit les éléments de base de toute PIA, ce qui démontre de la part des responsables américains un certain engagement quant à la nécessité de réaliser des PIA dans le contexte du secteur public américain et, plus concrètement, dans le cadre du développement du gouvernement électronique.
Le choix du législateur américain, qui a voulu créer un cadre légal *ad hoc*, capable de fournir un régime adapté aux exigences des programmes du gouvernement électronique, nous semble tout aussi intéressant.
Cette obligation de procéder à une PIA, processus équivalent aux ÉFVP, nous montre clairement une vision très axée sur la gestion du risque grâce à des mécanismes qui, à notre avis, aident vraiment à assurer une application effective des principes de protection des renseignements personnels.
Toutefois, cette loi américaine, qui cherche à encadrer le gouvernement électronique, présente une certaine complexité dans son application quand il s'agit de l'obligation de procéder à la réalisation des PIA. Ainsi, certains auteurs nous démontrent que, par exemple, cette loi ne s'applique pas dans tous les cas lorsque l'on traite de la problématique de l'inclusion des réseaux sociaux dans le débat citoyen-gouvernement dans les programmes de cybergouvernement où des risques liés à la protection des renseignements personnels des citoyens sont faciles à imaginer. D. Keats Citron affirme d'ailleurs :

> « *The E-Government Act does not apply to information generated on social-network sits if agencies decline to incorporate individual's social-network information to their data-bases. If, however, an agency*

[724] *E-Government Act, Public Law* 107-347, 44 U.S.C. ch. 36.

> *sistematically downloads the social-media data or more than ten people, it would be obliged to produce a privacy-impact-assesment report.* »[725]

La Commission européenne, dans sa communication de novembre 2010 « Une approche globale de la protection des données à caractère personnel dans l'Union européenne »[726], fait également référence aux « analyses d'impact au regard de la protection des données ». Dans cette communication, la Commission soulève toute une série de questions afin de savoir si la législation européenne en matière de protection des renseignements personnels va encore permettre de relever efficacement tous les défis contemporains.

Dans ce contexte, la Commission s'est donné pour objectif d'examiner certaines questions, notamment en vue de responsabiliser les responsables du traitement. Ainsi, une de ces questions est celle « d'introduire dans le cadre juridique l'obligation, pour les responsables du traitement, de réaliser une analyse d'impact au regard de la protection des données dans certains cas, par exemple lorsque les données sensibles sont traitées ou lorsque le type de traitement comporte des risques spécifiques, notamment dans le cas de l'utilisation de technologies, mécanismes ou procédures spécifiques, tels que le profilage ou la cybersurveillance »[727].

En effet, la position de la Commission européenne dans le contexte d'une réforme du régime actuel de protection des données personnelles est d'établir l'obligation juridique de procéder à cette analyse d'impact, qui équivaut aux ÉFVP, notamment dans les cas où des risques en raison de la sensibilité des renseignements personnels traités ou des technologies utilisées peuvent être identifiés.

Il faut noter que l'objectif est de donner à cette obligation force de loi, afin de s'assurer de que les organismes n'auront pas d'autre choix que se conformer à cette contrainte.

---

[725] D. KEATS CITRON, préc., note 681, p. A-118.

[726] COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS, préc., note 672.

[727] *Id*., p. 14 (nous soulignons).

P. Trudel avance le concept de une « gestion équitable des risques » comme un des impératifs de l'État de droit et affirme que, dans l'objectif d'assurer « le développement de systèmes d'information qui soient pleinement compatibles avec les exigences des lois, il paraît de plus en plus en plus nécessaire de mener une analyse globale des risques associés aux gisements de même qu'aux mouvements de l'information au sein des environnements réseautiques »[728].

Ces ÉFVP deviennent des outils nécessaires à la gestion du risque et dans un environnement en réseau, notamment, dans un État interconnecté, sont « effectués d'une manière proportionnée au niveau de risque déterminé avant l'établissement d'une activité ou d'un programme nouveau ou ayant subi des modifications importantes renfermant des renseignements »[729].
Il nous semble qu'appuyer d'une obligation légale la réalisation de ces processus d'ÉFVP, comme il est demandé au Canada et au niveau européen, peut aider à créer un cadre adapté et efficace pour les risques présents dans les environnements en réseau. C'est aux États-Unis que, dans le contexte d'une loi cherchant à encadrer le cybergouvernement, une obligation légale a été imposée par loi pour ce qui a trait à la réalisation des PIA dans le secteur public, ce qui démontre d'une certaine façon l'adaptation de cet outil à un tel contexte.

De plus, les ÉFVP que le Canada commence à utiliser depuis quelques années déjà, nous semblent à l'heure actuelle un des mécanismes pouvant être combiné à d'autres et ainsi contribuer à l'application effective des principes de protection, notamment celui de finalité. Cet outil peut aider à identifier clairement les risques qui découlent, par exemple, des partenariats public-privé existant dans le contexte du partage d'informations dans les projets de cybergouvernement.

Dans le cas canadien, il nous semble que ces mesures doivent servir à rééquilibrer la trop grande flexibilité que certaines dispositions de la LPRP, comme le

[728] P. TRUDEL, préc., note 222, p. 409.
[729] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 722.

paragraphe 8(2) de la LPRP, accordent aux organismes du secteur public pour partager des renseignements. En effet, les ÉFVP peuvent aider à neutraliser les risques pouvant découler des lacunes de la LPRP pour encadrer le modèle d'administration en réseau.

Il convient de noter également que le CPVPC a publié dernièrement un guide devant servir à la présentation des ÉFVP, qui apporte des informations importantes afin de faire la lumière sur le processus d'analyse en cours dans cette institution et d'exposer les attentes à l'égard des institutions fédérales à ce sujet.
Pour le CPVPC, il est essentiel que les entités fédérales prouvent que l'initiative ou programme est « nécessaire à l'atteinte d'un but précis et légitime, qu'il ou qu'elle a des chances d'être efficace dans l'atteinte de ce but, que l'atteinte à la vie privée est proportionnelle aux avantages qui en découleront et qu'aucun autre moyen qui porterait moins atteinte à la vie privée ne permettrait d'atteindre le même objectif »[730]. Afin de réaliser cette analyse, le CPVPC va répondre aux questions qui ont été posées dans *R.C. Oakes* – que nous avons étudié précédemment – et qui doivent servir à « évaluer les limites raisonnables des droits et libertés dans une société libre et démocratique »[731].

Bien sûr, les ministères et organismes vont devoir soumettre leurs rapports d'ÉFVP finaux au CPVPC avant de mettre en place les programmes et services en question et le CPVPC aura l'occasion de fournir des conseils et de proposer des alternatives pour ce qui relève des risques éventuels en matière de vie privée.

Plusieurs principes, tels que celui de responsabilité, de détermination des fins de la collecte des renseignements, de consentement, de limitation de l'utilisation, de la communication et de la conservation ou transparence régissent les ÉFVP. Le CPVPC mentionne parmi les principales étapes des ÉFVP le fait de déterminer où

[730] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 715, p. 6.
[731] *Id.*

les renseignements personnels sont envoyés après leur collecte ou de déceler les risques d'entrave à la vie privée et d'évaluer leur niveau.

Il nous semble crucial que cet instrument aide à garantir le fait que la protection de la vie privée doit être prise en considération, et cela au moment de la planification et de la mise en œuvre d'un projet dans le secteur public canadien.

Toutefois, nous considérons qu'aujourd'hui le cadre régissant les ÉFVP au Canada peut être renforcé. Les ÉFVP ne sont obligatoires au Canada que depuis 2002, conformément à une politique gouvernementale qui a été établie par le Secrétariat du Conseil du Trésor[732]. C'est-à-dire que l'obligation de procéder à ces démarches n'est pas contenue dans la LPRP ni dans aucune loi ou règlement en vigueur au Canada.

Toutefois, le CPVPC a proposé que le processus soit obligatoire en vertu de la loi et cela, suite à la réforme de la LPRP que le CPVPC demande depuis des années. De plus, même si le CPVPC appui une telle politique, il n'hésite pas à affirmer qu'elle serait sans doute plus efficace si elle avait force de loi[733].

Nous constatons que le SCT a remplacé la politique sur l'évaluation des ÉFVP de 2002 par une directive de 2010 qui veut être claire en la matière[734]. Cette directive est entrée en vigueur le 1er avril 2010 et elle constitue, à notre avis, un pas important dans la création d'un cadre capable de tenir compte des risques dérivés de la mise en place de services du gouvernement, tels que les prestations électroniques de services dans le contexte des réseaux gouvernementaux.

[732] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Commentaires présentés par Patricia KOSSEIM, préc., note 718.
[733] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 723.
[734] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 722.

Cette directive est entrée en vigueur le 1er avril 2010 et remplace l'ancienne politique du SCT sur les ÉFVP[735] datant de 2002, ainsi que les composantes qui portent sur le couplage des données de la politique sur la protection des renseignements personnels du SCT de 1993.

La Directive sur l'évaluation des facteurs relatifs à la vie privée établit un calendrier d'un an, jusqu'en avril 2011, pour que les institutions mettent en œuvre les différentes parties et exigences contenues dans cet instrument.

Cette directive sur les ÉFVP soutient les responsabilités du président du Conseil du Trésor, puisqu'elle veille à ce que, avant la mise en œuvre d'une activité ou d'un programme nouveau ou ayant subi des modifications importantes comportant des renseignements personnels, on puisse évaluer et régler correctement les questions ayant rapport à la vie privée.

En effet, le président du Conseil du Trésor du Canada à titre de ministre désigné en vertu du paragraphe 3.1(1) de la LPRP assume la responsabilité générale de l'enregistrement de tous les fichiers de renseignements personnels et examine comment ces fichiers sont gérés, comme le paragraphe 71(1) de la LPRP le prévoit.

Il est chargé d'examiner et d'approuver les nouveaux fichiers de renseignements ainsi que ceux qui ont subi des modifications importantes. Cette directive[736] sert à fournir aux institutions fédérales des directives sur la manière de réaliser les ÉFVP et d'assurer une « solide gestion et la prise de décisions judicieuses, ainsi qu'un examen prudent des risques liés á la vie privée dans le contexte de la création, de la collecte ou du traitement de renseignements personnels, dans le cadre d'activités ou de programmes gouvernementaux, en effectuant des ÉFVP ».

---

[735] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 523.

[736] Il faut noter que cette directive est publiée en conformité à l'alinéa 71(1)d) et aux paragraphes 71(3), 71(4), 71(5) et 71(6) de la LPRP.

La directive fournit une liste des cas où les organismes doivent amorcer une ÉFVP. Le SCT fait notamment référence au cas où des renseignements personnels sont utilisés dans le cadre d'un processus décisionnel concernant les citoyens. Mais nous pouvons encore citer les cas de sous-traitance, de transfert du programme ou d'activité à un autre niveau de gouvernement ou dans le secteur privé, ainsi que les cas où ce transfert provoque une modification importante du programme ou de l'activité.

Cette directive tient compte également des cas où plusieurs institutions sont impliquées dans un programme, ce qui déclenche une ÉFVP pluri-institutionnelle. Normalement, l'institution qui exerce le contrôle principal des renseignements personnels, ou qui est responsable du programme en question, sera responsable de la ÉFVP.

Si le programme est exécuté dans toutes les institutions fédérales, l'institution responsable de la ÉFVP va être en charge de certaines questions, notamment de superviser la collecte initiale ainsi que de toutes les divulgations à des institutions fédérales impliquées dans le programme ou activité.

Certains font remarquer que le SCT par cette directive a opté pour une « démarche fondée davantage sur le risque qui intègre la protection des renseignements personnels aux exigences en matière de responsabilité des gestionnaires supérieurs des services publics, et qui assure une surveillance de la conformité plus efficace »[737].

L'Annexe B de la directive contient les exigences en matière d'évaluation des facteurs relatifs à la vie privée concernant le processus de présentations au Conseil du Trésor. En effet, cette annexe édicte quelles sont les obligations des institutions fédérales qui demandent l'approbation du Conseil du Trésor pour des programmes

[737] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Commentaires présentés par Patricia KOSSEIM, préc., note 718.

ou des activités qui comportent des renseignements personnels. En effet, les institutions fédérales sont chargées de certaines tâches telles que faire tous les efforts raisonnables afin de faire commencer l'ÉFVP au stade initial de la planification du projet.

Cet annexe inclut une note qui rappelle aux institutions fédérales que la Politique sur la protection de la vie privée du SCT[738] oblige les responsables des institutions d'aviser le CPVPC de toute initiative – loi, règlement, politique ou programme – ayant un rapport avec la LPRP ou l'une de ses dispositions, ou pouvant avoir une incidence sur la vie privée.

L'Annexe C présente l'ÉFVP de base, qui regroupe des éléments standardisés de l'ÉFVP ayant un lien direct avec les obligations politiques et légales. Afin de mener une ÉFVP, il est nécessaire de compléter l'ÉFVP de base présente à l'annexe C, qui comprend 8 sections.

Les différentes sections et les informations que cette annexe présente constituent le contenu minimal d'une ÉFVP. La Section I tient compte de l'aperçu et de la tenue de l'ÉFVP.
La Section II est consacrée à l'identification et la catégorisation des secteurs du risque, partie qui, à notre avis, présente un intérêt particulier dans le cas des réseaux du gouvernement. Cette ÉFVP de base doit absolument contenir cette identification et catégorisation préliminaires des risques.

De plus, en voulant offrir une « approche uniforme » pour ce qui est des catégories des risques et des échelles de risques pangouvernementales, le SCT demande que les secteurs normalisés de risque, ainsi que les échelles de risque qu'ils présentent, soient maintenus comme base pour une analyse préliminaire du risque.

[738] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 325.

Nous constatons en effet une volonté d'offrir des éléments standardisés pouvant servir aux institutions afin de réaliser correctement ces ÉFVP, en fournissant un contenu minimal et en voulant garantir une certaine uniformité de base.
Pour cela, une échelle de risque chiffrée est présentée en ordre croissant pour le secteur en question. Ainsi, des questions telles que le type de programme, le type de renseignement, la participation des partenaires et du secteur public, la durée du programme ou la transmission des renseignements personnels sont analysées afin de déterminer la présence possible de risques et d'atteinte à la vie privée alors évalués et, parfois, atténués.

La Section III encadre l'analyse des éléments de renseignements personnels du programme ou de l'activité et la Section IV comporte les questions relatives aux flux des renseignements dans le cadre du programme, ce qui oblige pour ces ÉFVP à nommer les utilisations et divulgations internes et externes en indiquant plus particulièrement qui aura accès aux renseignements en question.

Cette section contraint également à nommer l'endroit où les renseignements circuleront ainsi que le lieu où ils seront détenus. Bien sûr, dans les cas des ÉFVP pluri-institutionnelles des obligations pour chacune des institutions sont requises pour ce qui relève du traçage des flux de renseignements pour les renseignements relevant de l'institution. L'institution fédérale responsable va devoir tracer le flux des renseignements entre les différentes institutions fédérales.

Finalement, la Section V fait référence à l'analyse de la conformité relative à la protection de la vie privée, où nous retrouvons pour la plupart des questions ayant trait au respect des différentes règles et principes de la LPRP. En effet, le SCT exige que l'analyse de la conformité relative à la protection des renseignements couvre les secteurs mentionnés à cet effet dans la politique et identifie les mesures précises de conformité prises ou à prendre pour chacun des secteurs en question. Ainsi, par exemple, nous retrouvons parmi ces secteurs l'autorisation de procéder à la collecte des renseignements conformément à l'article 4 de la LPRP, la

conservation des renseignements conformément à l'article 6 de la LPRP, l'usage des renseignements conformément à l'article 7 de la LPRP et la divulgation des renseignements conformément à l'article 8 de la LPRP.

Nous constatons alors que ces ÉFVP ont pour objectif, entre autres, de s'assurer du respect des principes de protection des renseignements personnels contenus dans la loi canadienne en la matière applicable au secteur public.

Il nous semble important de bien montrer que cet outil garde un lien étroit avec la LPRP, ce qui aide les institutions à respecter les dispositions du texte législatif en respectant le contenu minimal que cette ÉFVP de base présente.
Bien sûr, dans le cadre des structures en réseau, cet outil tient compte des particularités dans la circulation des informations et des risques attachés au contexte. De plus, cet ÉFVP de base offre une grille capable d'appréhender clairement les risques pouvant découler, par exemple, de la participation au programme en question d'autres institutions fédérales, provinciales ou même étrangères, ainsi que celles du secteur privé.

La question de savoir si les renseignements sont transmis à l'aide de technologies sans fil ou celle qui cherche à déterminer si les renseignements sont utilisés au sein d'un système fermé sont deux questions visées par l'ÉFVP de base, ce qui est fortement utile à l'heure d'analyser les risques des projets dans le cadre, notamment, d'un gouvernement électronique ou d'une prestation électronique de service.

Il nous semble important d'étudier dans les années à venir quel sera l'impact d'une telle directive et si, effectivement, les institutions fédérales vont répondre à l'obligation imposée par un tel outil et présenter les ÉFVP suite à l'approbation officielle conformément au processus d'approbation de l'institution fédérale en question.

Cette question nous intéresse particulièrement, de même que le rôle que joueront le SCT et le CPVPC dans ce contexte. Si le CPVPC est en mesure de déterminer le niveau d'analyse et de demander qu'on lui fournisse tous les renseignements et la documentation supplémentaire sur un programme ayant un impact sur la vie privée des Canadiens, il reste à voir quel sera le vrai pouvoir suite à une ÉFVP. Bien sûr, tout organisme, au moment de soumettre le modèle approuvé d'ÉFVP au SCT doit s'assurer d'en fournir une copie au CPVPC et lui remettre tous les documents demandés.

Les organismes doivent soumettre les rapports d'ÉFVP finaux au CPVPC, et cela avant de mettre en œuvre les programmes ou services. Par la suite, le CPVPC va seulement pouvoir fournir des recommandations ou émettre des commentaires à l'égard des institutions.

Il nous semble décisif de signaler que la décision finale sur la possible mise en œuvre de ces recommandations ou commentaires appartient uniquement et exclusivement aux organismes en question[739].

C'est pourquoi nous nous demandons si, dans le cas où le CPVPC manifeste des doutes par rapport à un nouveau programme ou à un changement dans une activité déjà existante à cause de risques potentiels pour la vie privée, cette autorité a vraiment le pouvoir d'éviter la mise en place de telles mesures. C'est, à notre avis, une des questions essentielles concernant l'efficacité de ces mesures et l'impact de l'action du CPVPC dans les programmes et activités comportant des renseignements personnels dans le secteur public canadien.

**2- Le respect de la vie privée dès la conception ou la *Privacy by Design***

Le *Privacy by Design* est devenu une notion de plus en plus importante dans le cadre de la protection des renseignements personnels. Le respect de la vie privée dès la conception peut contribuer à la responsabilisation, comme le Contrôleur

[739] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 723.

européen l'a souligné : « *Accordingly to the EDPS privacy by design is an element of accountability* »[740].

Lors de la 32e Conférence internationale des commissaires à la protection des données et à la vie privée de 2010, une résolution sur la *Privacy by Design*[741] a été adoptée par l'ensemble des autorités de contrôle, ce qui suppose la reconnaissance du *Privacy by Design* comme une composante essentielle de la protection de la vie privée.

Les promoteurs d'une telle résolution expliquent comment et pourquoi ce concept a été développé :

> « *The concept of "Privacy by Design" was developed to address the ever-growing and systemic effects on Information and Communications Technologies (ICT), and of large-scale networkedinfrastructure, in a comprehensive manner. Privacy by Design refers to the philosophy and approach embedding privacy into design, operation and management of information technologies and systems, across the entire information life cycle.* »[742]

Nous observons alors que cette notion s'inscrit parfaitement dans des mécanismes capables d'encadrer la protection des renseignements personnels dans des structures en réseau à grande échelle, et cela pendant tout le cycle de vie des informations. C'est pourquoi cet outil nous semble indispensable dans la conception de la protection de la vie privée devant prévaloir dans les réseaux de l'administration et plus particulièrement dans le contexte du cybergouvernement.

---

[740] CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, préc., note 675, p. 23.
[741] 32ND INTERNATIONAL PRIVACY OF DATA PROTECTION AND PRIVACY COMMISSIONERS, *Privacy by Design Resolution*, 27-29 Octobre 2010, Jerusalem, Israel, en ligne : www. privacybydesign.ca ( consulté le 12 mars 2011).
[742] *Id.*, (nous soulignons).

Le Contôleur européen affirme en janvier 2010 : « *Privacy by Design refers to the integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data* »[743].
En effet, *Privacy by Design* s'inscrit dans l'idée que le futur du droit à la protection de la vie privée passe par le recours à d'autres outils de protection que les lois en la matière : « *Regulation and policy are no longer sufficient to safeguard privacy* »[744].
En raison de cette incapacité des instruments purement législatifs à encadrer la protection de la vie privée aujourd'hui, il est nécessaire de nous tourner vers l'idée d'une protection se trouvant directement dans les systèmes de gestion des renseignements personnels : « *With the increasing complexity and interconnectedness of information technologies, nothing short of building privacy directly into system design and processes can suffice* »[745].

Parmi les sept principes[746] sur lesquels s'appuie la *Privacy by Design*, il nous semble que celui du *Privacy as the Default Setting* est d'une grande importance, puisqu'il assure que même si la personne concernée n'a pas une attitude active en vue de protéger la confidentialité de ses données, le système assure cette protection, puisque celle-ci est intégrée dans le système. Ainsi, il est intéressant de constater que les théoriciens du *Privacy by Design* soulignent que ce principe du *Privacy as the Default Setting* s'appuie spécialement sur des principes tels que celui de finalité[747]. Cas intéressant, puisque nous pouvons imaginer des systèmes ou des projets dans lesquels, par défaut, tout est fait pour assurer le respect du principe de finalité par rapport aux renseignements personnels en question.

---

[743] CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, préc., note 675, p. 23.
[744] 32ND INTERNATIONAL PRIVACY OF DATA PROTECTION AND PRIVACY COMMISSIONERS, préc., note 741.
[745] *Id*.
[746] Ann CAVOUKIAN, *Privacy by Design* : *The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices*, 20 août 2009, en ligne : "http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf" ( consulté le 11 avril 2011).
Ce document présente ces 7 principes : 1. *Proactive not Reactive- Preventive not Remedial* ; 2. *Privacy as the Default Setting*; 3. *Privacy Embedded into Design*; 4. *Full Functionality- Positive-Sum, not Zero-Sum*; 5. *End-to-End Security-Lifecycle Protection*; 6. *Visibility and Transparency*; 7. *Respect for User Privacy*.
[747] *Id*.

De plus, il est affirmé que, dans les cas où le besoin d'utiliser des renseignements personnels n'est pas clair ou justifié, le « principe de précaution » doit être appliqué et la « présomption de vie privée » privilégiée, par un système qui puisse garantir cette protection.
La résolution sur *Privacy by Design*, adoptée par l'ensemble des autorités de protection des données personnelles fait appel à ces autorités pour qu'elles incluent les « *Foundational Principles* » du *Privacy by Design* dans la formulation des politiques de vie privée et dans la législation en matière de protection des renseignements personnels dans leurs respectives juridictions.

Dans le contexte européen, le Contrôleur européen a proposé en janvier 2011 que le principe du *Privacy by Design* se trouve parmi les principes directeurs devant guider le processus de révision du cadre juridique européen, ainsi que l'introduction de dispositions générales à ce sujet[748].

En effet, le Contrôleur européen affirme que la Directive 95/46/CE, même si elle contient quelques dispositions qui encouragent le *Privacy by Design*, ne comprend aucune obligation explicite à cet effet.
Voici ce que le Contrôleur propose pour inclure une obligation légale au niveau européen sur les exigences de la part des autorités de protection en ce qui concerne le respect des principes du *Privacy by Design* :

> « *The EDPS is pleased with the Communication's endorsement of privacy by design as a tool towards ensuring compliance with the data protection rules. He suggests including a binding provision setting forth a "privacy by design" obligation, which could build on the wording of Recital 46 of Directive 95/46. More specifically, the provision would explicitly require data controllers to implement technical and organization measures, both at the time of the design of the processing itself, particularly in order to ensure the protection of personal data and prevent any unauthorized processing.* »[749]

[748] CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, *Communiqué de presse sur la « Stratégie de réforme de la protection des données : le CEPC présente sa conception du nouveau cadre juridique »*, Bruxelles, mardi 18 janvier 2011.
[749] CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, préc., note 675, p. 23.

Nous constatons alors l'existence de l'idée de plus en plus repandue selon laquelle ce principe du *Privacy by Design* est un outil à mettre en place en vue de s'assurer que les systèmes et les projets sont construits depuis le début en ayant comme base le respect de la privée privée.
Cette conception de la protection de la vie privée, ayant recours à des mécanismes qui servent d'une certaine façon à une application du principe de précaution, va permettre de mettre l'accent sur la prévention de certains problèmes, et cela avant la mise en place des systèmes et des programmes.
Les ÉFVP et le *Privacy by Design* sont des outils qui doivent être combinés à d'autres solutions techniques et législatives en vue de protéger la vie privée dans le contexte actuel, caractérisé par une compléxité qui nécessite une telle solution de protection.

Nous observons pourtant également des voix qui demandent d'inclure, dans les textes législatifs actuels, dans le contexte de réformes futures, des dispositions qui obligent à mettre en place ces processus et mesures. Le besoin de donner force de loi aux obligations liées aux ÉFVP et au principe du *Privacy by Design* témoigne de la nécessité du caractère obligatoire que la loi impose et qui peut servir à créer le cadre le mieux adapté aux environnements en réseau.

### 3- Gouvernance des réseaux basée sur la notion de « contrôle » de l'information et sur la mise en place de solutions techniques

Nous observons dans les structures en réseau que différentes formes d'échange, de cession et de transmission de l'information existent. En effet, dans un réseau, l'information a tendance à circuler, mais il faut savoir identifier les différents « gestes », du simple transit de l'information à l'appropriation de cette information, puisque toutes ces opérations sont différentes.
En effet, certains organismes peuvent jouer le rôle de simples dépositaires des informations, tandis que d'autres organismes ont le pouvoir d'accéder à l'information, de l'utiliser et même de communiquer les renseignements personnels.

Penser que toutes ces opérations répondent à la même logique et qu'elles sont équivalentes et similaires, risque d'engendrer une vision limitée de la complexité que les structures en réseau renferment.

En effet, dans un réseau, il faut également tenir compte de la notion de « contrôle » afin de comprendre que le contrôle complet ou partiel de l'information détermine les responsabilités en matière de protection des renseignements personnels. En considérant le degré de l'intensité du contrôle exercé sur un document, on peut développer le cadre juridique qui doit déterminer les droits et responsabilités dans le contexte du réseau[750].

V. Gautrais et P. Trudel proposent la notion d'échelle de contrôle sur les documents au moment d'identifier les différentes responsabilités dans les structures réseautiques. Pour ces auteurs, cette « échelle mobile » concerne le droit d'accès aux informations mais également l'ensemble des autres relations pouvant exister « entre un acteur donné et l'information qui transite dans un réseau »[751]. Ainsi, ils signalent que plus on a le contrôle d'un document, plus on répond de la protection des informations en question.

Voici l'idée qui dissocie les notions de contrôle de l'information et de possession physique du support d'une telle information : « Dans un réseau, l'information qui circule n'est pas nécessairement sous l'entier contrôle de l'entité qui se trouve à avoir la possession physique du support »[752].

À notre avis, cette vision de la question de l'accès à l'information dans le contexte du réseau basé sur le contrôle peut aider à créer un cadre réaliste et capable de gouverner convenablement les structures en réseau.

La séparation réalisée entre support et information aide effectivement à imaginer une répartition des responsabilités dans un contexte réseautique. De plus, nous devons tenir compte de l'idée selon laquelle, dans un réseau et dans le monde

[750] V. GAUTRAIS et P. TRUDEL, préc., note 143, p. 69 et s.
[751] *Id*., p. 70.
[752] *Id*., p. 16.

physique ou non virtuel, même si l'information circule entre les mains de plusieurs acteurs ayant pour mission de transférer les informations, ces acteurs n'ont sur celle-ci qu'un contrôle physique, à l'image de celui exercé par le facteur pendant le processus de livraison d'une lettre, processus pendant lequel il ne peut pas prendre connaissance de son contenu[753].

À notre avis, les mesures techniques doivent être capables d'encadrer ces rapports au support et aux informations des différents intervenants ou organismes publics opérant dans le réseau, et cela en fonction des responsabilités et des droits d'accès des acteurs.

Dans ce contexte, la question importante n'est pas tellement de savoir qui est en possession des informations, mais plutôt qui a le droit d'y accéder et d'en faire usage[754], notamment pour prendre une quelconque décision administrative concernant les citoyens.

Cette vision va également déplacer la question du principe de finalité dans le contexte du réseau. Pour P. Trudel, ce n'est plus en regard de la « détention » de l'information que s'applique l'exigence du respect de la finalité mais plutôt en regard de l'accès et de l'utilisation qui sera faite du renseignement[755].

Par conséquent, nous considérons que, en vue de garantir l'application du principe de finalité dans les environnements en réseau du secteur public, la gestion de l'accès aux informations par les différents acteurs du réseau est essentielle.

Ainsi, les mesures techniques peuvent servir à encadrer toutes les opérations relatives à l'information. La catégorisation des informations et la détermination des acteurs pouvant accéder, communiquer ou même utiliser les informations, doit servir au schéma de gouvernance prévalant dans les environnements en réseau.

---

[753] Voir à cet effet : *Id*., p. 71.

[754] Pierre TRUDEL, « Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *Revista Catalana de Dret Public*, num. 35, 2007, 247, 250.

[755] *Id*., 264.

Les opérations identifiables dans le contexte de la circulation des renseignements personnels trouvent normalement leur origine dans le texte des instruments législatifs en matière de protection des données personnelles. Ainsi, les termes « communication », « conservation », « détention », « donner accès », « possession », « transmission » ou « utilisation », entre autres, témoignent des différentes opérations existant dans le contexte québécois et canadien[756].

Le régime de responsabilité des différents intervenants dans le déroulement de ces opérations doit aider à mettre en place les mesures de sécurité nécessaires afin de protéger convenablement les renseignements personnels.

Dans le cas de l'Espagne, nous observons que des différences importantes existent entre « l'accès automatisé », la « simple interconnexion » ou la « communication », ce qui requiert une gestion des accès *ad hoc* afin d'assurer la protection des renseignements personnels dans le cadre des différentes opérations[757].

Nous retrouvons également des concepts tels que le « partage des données », notion différente de celle de la « comparaison informatisée »[758], qui démontrent la complexité entourant les termes utilisés et les caractéristiques de l'ensemble des opérations touchant à la circulation des informations.

De plus, dans le contexte de l'impartition et des partenariats public-privé, les notions de « contrôle » et de « garde » deviennent très importantes afin d'établir correctement la responsabilité des organismes publics et des entreprises privées dans la gestion de l'information[759].

Dans ce contexte, où le degré de contrôle pouvant être exercé sur les informations et la capacité des différents organismes à communiquer ou utiliser des informations

---

[756] V. GAUTRAIS et P.TRUDEL, préc., note 143, p. 226 à 231.
Voir le « tableau récapitulatif des opérations susceptibles de survenir lors de la circulation de renseignements personnels » que ces auteurs nous présentent.

[757] Voir à ce sujet: Julián VALERO TORRIJOS et Manuel FERNÁNDEZ SALMERÓN, « Protección de datos y Administración electrónica », *Revista Española de Protección de datos*, Juillet-Décembre 2006, I, 115, 134.

[758] Voir : COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, *Perspectives*, Vol. 5, n° 2, Printemps 2006, 6.

[759] D. H. FLAHERTY, préc., note 262, p. 25.

deviennent des facteurs importants, des solutions techniques peuvent aider à assurer la gouvernance des réseaux.

Voici l'idée que J.R. Reidenberg et P.M. Schwartz avancent sur la manière dont les solutions techniques peuvent être à l'origine des moyens à mettre en place en vue de protéger la vie privée : « *Just as technology may be part of the problem for data protection, the technological infrastructure may also form part of the solution* »[760].

De plus, à l'intérieur même des institutions, les systèmes, par leur architecture, doivent être capables d'encadrer l'accès aux informations selon les autorisations accordées aux différents acteurs.

Dès nos jours, nous pouvons imaginer des systèmes pouvant empêcher la multiplication et la copie de l'ensemble des informations, ou envisager l'implantation de systèmes qui ne vont pas permettre d'accéder à l'ensemble des informations, mais uniquement offrir la simple possibilité, pour un organisme du secteur public, d'aller vérifier une information dans les banques de données détenues par un autre organisme.

Dans le contexte de l'Union européenne, le Groupe de l'article 29 et le Groupe de travail « Police et Justice » soulignaient en décembre 2009 l'importance de l'architecture de tout système de stockage de données personnelles et signalaient notamment que « l'accès à d'importantes bases de données doit être configuré de sorte à interdire, de manière générale, la consultation directe en ligne des données stockées, et un système "trouvé/non trouvé" ou dispositif d'indexation est généralement jugé préférable »[761].

---

[760] Joel R. REIDENBERG et Paul M. SCHWARTZ, *Data protection law and on-line services : regulatory responses*, Étude préparé dans le cadre du projet « Vie privée et société de l'information : Étude sur les problèmes posés par les nouveaux services en ligne en matière de protection des données et de la vie privée », commandé à ARETE par la DG XV de la Commission Européenne, Bruxelles, 1998.

[761] GROUPE DE TRAVAIL « ARTICLE 29 » ET GROUPE DE TRAVAIL « POLICE ET JUSTICE », *L'avenir de la protection de la vie privée*, Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, adoptée le 1er décembre 2009, p. 31.

Bien sûr, dans le cadre des prestations électroniques des services où la mise en commun des différentes informations détenues par plusieurs organismes peut s'avérer nécessaire, des solutions technologiques capables de limiter les accès, les utilisations et les communications des renseignements personnels peuvent apporter des solutions importantes.

Regardons comment J.R. Reidenberg et P.M. Schwartz envisagent l'utilisation de solutions techniques en vue d'assurer l'utilisation des renseignements personnels uniquement pour des fins compatibles avec celles ayant motivé la collecte : « *An infrastructure may be designed to assure that only relevant information be collected when "identified or identifiable" information is required or may be structured to preclude any processing other than purposes compatible with the original goals for the collection* »[762].

Ces auteurs apportent une réflexion intéressante sur les possibles conflits provenant des différences entre les lois en matière de protection des renseignements personnels des différents pays.

Ils font concrètement référence au contexte européen, mais nous pouvons parfaitement imaginer pareille situation entre les lois canadiennes, américaines ou européennes : « *To some extent, technological solutions may be able to minimize any conflicts over some of the divergences in the laws of the Member States* »[763].

Dans le contexte des échanges de données entre organismes, même à l'extérieur des frontières, nous imaginons effectivement que les solutions techniques peuvent apporter des éléments pouvant assurer une protection équivalente durant tout le cycle de vie des informations, indépendamment de la nature des flux dont ils feront l'objet.

En effet, en fonction du type de contrôle exercé sur les informations par les différentes institutions opérant dans les réseaux du secteur public, des solutions techniques *ad hoc* peuvent être envisagées afin d'assurer une protection maximale

[762] J. R. REIDENBERG et P. M. SCHWARTZ, préc., note 760 (nous soulignons).
[763] *Id.*

en matière de vie privée. Bien sûr, la mise en place de ces solutions techniques en fonction du degré de contrôle sur l'information devrait être envisagée durant l'étape de la conception du système, en suivant les principes que la *Privacy by Design* préconise.

Ainsi, toute la potentialité de la notion de contrôle de l'information en tant que concept-clé dans la gouvernance des réseaux et la mise en place de solutions techniques appropriées pourront servir à l'application effective des lois en la matière et, plus particulièrement, des principes de protection des renseignements personnels.

L'identification des différentes opérations concernant les informations et pouvant survenir dans les réseaux est essentielle. En dissociant par exemple, la garde, le contrôle, l'usage et le reste des opérations, nous arrivons à voir plus clair en ce qui concerne les responsabilités des différents acteurs du réseau.
Les mesures techniques assurant un accès pertinent aux informations en fonction du degré de contrôle pouvant être exercé par les différents acteurs peuvent aider à la création d'un cadre *ad hoc* pour protéger les renseignements dans les réseaux.

### 4- Le droit fondamental à la protection de la confidentialité des systèmes informatiques ou *Computer Grundrecht*

C'est en 2008 que la Cour constitutionnelle allemande a dû se positionner à propos de perquisitions secrètes en ligne réalisées par des agences gouvernementales. Plus concrètement, cette Cour constitutionnelle de Karlsruhe a déclaré contraire à la Constitution un amendement à la loi sur les renseignements personnels du Land de Rhénanie-du-Nord-Westphalie[764].

Si cette décision est significative, c'est qu'en effet elle pionnière puisqu'elle institue un nouveau « droit fondamental à la protection de la confidentialité et de

[764] *Cour constitutionnelle fédérale allemande, Arrêt du 27 fèvrier 2008.*

l'intégrité des systèmes techniques ou informatiques », et cela « comme élément des droits généraux de la personne dans la constitution allemande »[765].

Ce droit que certains qualifient de « droit fondamental des systèmes d'information »[766] change considérablement le paysage juridique car : « La Cour Constitutionnelle a donc précisé que le "droit général de la personnalité" doit être assorti d'une autre interprétation donnant naissance à un nouveau droit fondamental : le "droit à la garantie de la confidentialité et de l'intégrité des systèmes TIC" »[767].

Le Groupe de l'article 29 fait référence à cette jurisprudence allemande et à la création de ce nouveau droit constitutionnel :

> « Les systèmes capables de créer, de traiter ou de stocker des données sensibles à caractère personnel requièrent une protection particulière. Le champ de protection du droit fondamental à la confidentialité et à l'intégrité des systèmes d'informations s'étend aux systèmes qui, seuls ou du fait de leur interconnectivité technique, peuvent contenir des données à caractère personnel sur la personne concernée, à un degré et dans une diversité tels que l'accès aux systèmes fournit des informations sur des éléments importants de la vie de telle personne ou dresse un portrait révélateur de sa personnalité. Ces systèmes sont par exemple les ordinateurs personnels et les ordinateurs portables, les téléphones portables et les agendas électroniques. »[768]

Ainsi, nous observons que ce droit s'étend aux machines et aux systèmes, qui sont susceptibles de protection par le biais de ce droit fondamental assurant leur confidentialité et leur intégrité. Le Groupe de l'article 29 fait référence à cette

---

[765] Stefano RODOTA, « Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives », *Mouvements des droits et des idées, « Sous contrôle, gouverner par les fichiers »*, nº 62, avril-juin 2010, 56, 60.

[766] Danièle BOURCIER, *Les allemands et les Français face à la vie privée, que nous apprend le droit sur les cultures?*, Actes du 41e Congrès du Mouvement du jeune notariat, du 6 au 10 octobre 2010, p. 3.

[767] *Id.*, p. 8.

[768] GROUPE DE TRAVAIL « ARTICLE 29 » ET GROUPE DE TRAVAIL « POLICE ET JUSTICE », préc., note 761, p. 15.
Nous retrouvons cet extrait à la note de pied de page 13, en faisant référence dans le corps du texte à la jurisprudence allemande récente.

jurisprudence allemande en évoquant le principe de la prise en compte du respect de la vie privée dès la conception ou *Privacy by Design*, puisqu'il considère que les TIC doivent être conçues et développées afin d'éviter ou du moins limiter le nombre de données personnelles traitées[769]. Pour le Groupe de l'article 29, le *Privacy by Design* devrait imposer la mise en œuvre de la protection des données dans les TIC, conçues pour le traitement des données.

S. Rodota affirme que « les changements qu'engendrent la science et la technologie entraînent des transformations de la structure anthropologique et de la notion même d'humanité »[770]. C'est dans ce contexte évoqué par le juriste italien que nous considérons d'une grande importance l'apport de la jurisprudence allemande avec la création de ce nouveau droit.

> « La confidentialité, une qualité propre aux êtres humains, est ainsi accordée à la machine, reconnaissant par-là même qu'il n'y a pas seulement des interactions entre l'homme et la machine, mais une influence réciproque. La loi réaffirme ainsi la priorité accordée aux humains, et manifeste également sa puissance en nous disant que le monde entre dans une nouvelle phase, formée de la personne et l'appareil technique auquel elle confie des données. »[771]

Cette idée puissante, évoquée par S. Rodota nous semble importante et novatrice. Elle est réaliste, actuelle et en adéquation avec le nouveau contexte caractérisé par l'énorme place que les technologies de l'information occupent dans nos vies. De plus, elle est capable de montrer que ce nouveau droit fondamental en vigueur en Allemagne souligne davantage la grande interaction entre l'homme et la machine et la manière dont le droit doit être capable de tenir compte de cette intense relation.
En effet, c'est la Cour constitutionnelle qui a compris que cette étendue de la protection accordée par le droit doit parvenir à tenir compte de l'unité formée par l'humain et les machines auxquelles il confie ses renseignements.

[769] *Id.*, p. 15.
[770] S. RODOTA, préc., note 765, 59.
[771] *Id.*, 60 (nous soulignons).

Si Rodota parle de « continuum » entre la personne et la machine, il le fait en soulignant l'idée de la création d'une « nouvelle anthropologie qui impacte les classifications légales et change leur nature »[772].

D. Bourcier n'hésite pas à affirmer l'importance de ce nouveau droit comme voie pour la construction d'un nouveau cadre juridique en matière de vie privée : « Mais, la généralisation d'un droit fondamental pour le citoyen en matière de vie privée et d'informatique (*Computer Grundrecht*) à la hauteur des enjeux actuels pourrait bien devenir la future étape de la construction d'un droit européen dans ce domaine »[773].

Il nous semble en effet, que ce nouveau droit fondamental représente une vision de la problématique de la protection de la vie privée qui peut vraiment encadrer la réalité du réseau.

**5- Des nouvelles notions pouvant opérer dans les réseaux du gouvernement**

Des notions telles que les « aires de partage » ou les « enclaves protégées » ouvrent des perspectives intéressantes dans le domaine de la protection de la vie privée dans les réseaux du secteur public.

P. Trudel a introduit dans le débat relatif à la protection des données personnelles dans l'État en réseau, le concept d'aire de partage qui est définie ainsi :

> « L'aire de partage peut être définie comme un environnement d'information dans lequel les données personnelles nécessaires à la délivrance d'un ensemble de services accomplis au bénéfice des citoyens peuvent être rendus disponibles à différentes entités. Ces services ou prestations ont un caractère complémentaire et leur accomplissement nécessite des informations détenues par une pluralité d'entités liées par une entente. »[774]

[772] *Id.*
[773] D. BOURCIER, préc., note 766, p. 8.
[774] P. TRUDEL, préc., note 130, 263.

C'est, à notre avis, une notion très utile pour aider à la gouvernance des structures en réseau où les différents organismes du secteur public doivent parfois accéder à des renseignements personnels détenus par plusieurs entités en vue d'offrir des prestations aux citoyens.
Pour P. Trudel, ce concept renvoie à des mécanismes capables d'encadrer la circulation des informations, de délimiter les usages et d'avoir pour résultat un régime définissant les droits et responsabilités des acteurs du réseau.

Le processus de création de ces aires de partage doit assurer la légitimité des usages des renseignements personnels, raison pour laquelle un processus à caractère public est nécessaire avant leur mise en place. Ainsi, l'instauration de ces aires doit être nécessairement précédée d'un processus de concertation : « Le processus public assure la transparence et l'évaluation publique et contradictoire des enjeux et des risques »[775]. De plus, ce processus « vise à poser ouvertement les enjeux, les avantages et les précautions relatifs aux prestations électroniques envisagées et aux partages de renseignements qui sont projetés »[776].
Nous constatons alors que la transparence et le jugement de tous les acteurs impliqués devant les risques en matière de vie privée deviennent des éléments clés de la légitimité de ces espaces de partage des informations au sein des environnements électroniques du secteur public.
Pour ce qui est de l'encadrement juridique des aires de partage, il est clair que le respect des principes fondamentaux en matière de protection des renseignements personnels doit être assuré[777].

D.H. Flaherty, en évoquant la nécessité d'une gestion des renseignements personnels dans le cadre des services du gouvernement électronique, fait référence à une notion en particulier. Ainsi, il évoque la notion d'« enclave protégée » pouvant opérer dans le réseau du secteur public sous certaines conditions :

[775] *Id*., 264.
[776] *Id.*, 263.
[777] Voir : P. TRUDEL, préc., note 12, 554.

> « Si toutes les lois pertinentes orientées vers la protection de la vie privée et leur mise en œuvre connexe étaient vigoureuses, une enclave protégée pourrait échanger des renseignements avec une autre enclave protégée, dans des conditions contrôlées, à des fins gouvernementales légitimes et autorisées. »[778]

Ainsi, cet auteur envisage comme condition à ces échanges contrôlés entre enclaves protégées dans le cadre de l'administration à des fins gouvernementales légitimes, que les lois et leur mise en œuvre soient vigoureuses et que d'une certaine façon elles soient capables de protéger les renseignements personnels.

De plus, il considère que ces échanges entre enclaves protégées peuvent contribuer à la transparence dans le contexte des prestations de services dans l'administration : « Les ententes de partage des données donneraient au plublic la satisfaction de savoir que le Parlement, les organes législatifs et les chiens de garde de la vie privée ont une bonne idée de ce qui se déroule sur le plan des échanges de données pour la prestation des services (cela implique le secteur privé ) »[779].

Nous constatons alors que ces auteurs parlent de « mécanismes de nature consensuelle »[780] et qu'ils présentent ces possibles solutions dans le cadre du respect du critère des finalités d'utilisation des renseignements personnels. Même si ces deux solutions reposent sur des opérations et structures différentes, elles constituent de véritables moyens pour encadrer la question de la protection des renseignements personnels dans l'État en réseau. De plus, ces mécanismes peuvent être capables de neutraliser certains risques associés à l'échange de données entre les organismes du secteur public.

Dans la pratique, les « aires de partage » peuvent être encadrées de la manière suivante :

> « En tant qu'espace régulé, l'aire de partage est nécessairement balisée par les finalités de la famille des services et prestations pour lesquelles elle est établie. Le citoyen est informé de sa vocation, de sa

[778] D. H. FLAHERTY, préc., note 262, p. 20 (nous soulignons).
[779] *Id.*
[780] *Id.*

> portée et de sa teneur. Une liste des usages possibles des informations est continuellement disponible en ligne ou autrement. Ces espaces de circulation sont normés par les protections physiques et logiques de même que par les droits et autorisations d'accès. »[781]

En effet, les finalités d'utilisation des renseignements personnels détermineront la manière dont la gouvernance de ces aires sera établie et arrêteront ainsi leur architecture protectrice visant à permettre exclusivement les accès autorisés.
De plus, les fins seront fixées par les services offerts aux citoyens : « Si les Canadiennes et les Canadiens veulent des services particuliers, ils prendront la décision pragmatique de consentir à la collecte, à l'utilisation, à la communication et à la conservation des renseignements personnels à de telles fins »[782].
Il nous semble que la gouvernance des réseaux du gouvernement peut profiter de ce type de mécanismes, capables de rendre possible la prestation électronique de services offerts aux citoyens et de protéger les renseignements personnels ayant fait l'objet d'échange et d'utilisation. Ces pistes offrent des possibilités de protection basées sur les principes de protection des renseignements personnels fixés dans les lois en la matière et sont imprégnées d'une vision réaliste des enjeux que les réseaux gouvernementaux présentent. De plus, ils peuvent contribuer à l'application effective des lois en la matière, et notamment du principe de finalité.

Dans le contexte américain, A.B. Serwin propose la *Privacy 3.0*, basée sur le principe de proportionnalité :

> « (...) *the overarching principle of privacy of today should not to be the right to be alone, but rather the principle of proportionality. This is privacy 3.0.* »[783]

Il nous semble que, dans le contexte nord-américain et principalement dans celui des États-Unis, ce modèle présente des caractéristiques pouvant offrir un degré de protection important pour les informations circulant dans les réseaux. Ainsi, A.B.

[781] P. TRUDEL, préc., note 130, 264.
[782] D. H. FLAHERTY, préc., note 262, p. 20.
[783] A. B. SERWIN, préc., note 668, 899.

Serwin explique que dans les années à venir les entités opérant dans le contexte des soins de santé vont devoir se conformer à un modèle qui permettra d'échanger de façon électronique des informations de nature médicale.
De plus, aujourd'hui, dans le contexte qu'il qualifie de « Monde Web 2.0 » caractérisé par le partage instantané d'une énorme quantité d'informations relatives à la vie privée des gens, il est évident que rien n'est plus étranger à ce contexte que le concept du « *right to be alone* »[784]. Ce modèle de protection semble dès lors plus adéquat pour d'encadrer les structures en réseau où les informations circulent.

Pour cet auteur, la *Privacy 3.0* est basée sur ce principe de proportionnalité : « *The principle of proportionality recognizes that neither the government nor private citizens benefit (and in fact they have much to lose ) from overbroad privacy restriction* »[785].
Cette théorie de protection fondée sur la proportionnalité est basée sur l'établissement de grandes restrictions et de barrières d'accès protégeant les informations les plus sensibles, en limitant l'accès et l'utilisation de ces informations par des tiers. Il semble essentiel également de permettre un accès nécessaire et adéquat à ceux qui ont un besoin légitime de connaître certaines informations, notamment les moins sensibles.
Pour cela, ce système de protection est basé sur quatre niveaux de classification de l'information, classification conformant l'élément essentiel de cette théorie relative à la protection de la vie privée puisque cet auteur affirme que le principe de proportionnalité va devoir être appliqué et utilisé afin de créer ces catégories.

Ainsi, le niveau de sécurité et de confidentialité associé à chaque catégorie de l'information va dépendre de la sensibilité des renseignements ainsi que des méthodes pouvant être mises en place afin de recueillir, traiter et utiliser les informations en question. Voici les quatre niveaux proposés dans le cadre de cette

[784] *Id.*, 872.
[785] *Id.*, 875.

théorie : *highly sensitive information, sensitive information, slightly sensitive information* et *non-sensitive information*.

De plus, cette théorie va servir à ne pas empêcher ou limiter de façon générale le partage ou la circulation des informations, question de grande importance dans le contexte des réseaux :

> « *The advantage of the tiers created by the application of the principle of proportionality is the incorporation of a principle-based approach in a way that does not operate to stifle information sharing as some current principle-based approaches do, while simultaneously defining permissible and non-permissible actions based upon the tier within which the information falls, even in the absence of a specific statutory guidance. Thus, even if the law regarding a particular form of information is unclear or non-existant, a company seeking guidance in an uncharted area can assess its conduct by comparing what is permitted with other similar forms of information. This approach also provides clarity regarding underwippings of existing laws and guidance regarding future laws that will be necesary as new types of information and information sharing become more ubiquitous.* »[786]

En effet, cette théorie va aider à l'encadrement des modalités de partage des informations, au lieu d'empêcher par principe leur circulation et sera capable de donner des solutions adaptées aux nouveaux types de renseignements et aux nouvelles modalités de partage.

Voilà pourquoi il nous semble que ce système peut représenter un modèle « réseautique » d'encadrement, sans oublier que comme A.B. Serwin l'a souligné, ce cadre basé sur la proportionnalité va être spécialement utile puisque, grâce au système basé sur les quatre niveaux de sensibilité des informations, il sera en mesure de s'adapter aux changements opérant sur les normes ou les valeurs de la société[787].

---

[786] *Id.*, 900 et 901 (nous soulignons).

[787] *Id.*, 876.
L'auteur souligne que « the proportionality framework could also address more easily the changes in societal norms and values ».

Il s'agit, à notre avis, d'un modèle très pertinent pour la gouvernance des architectures réseautiques et d'une méthodologie particulièrement adéquate pour un contexte, comme celui du gouvernement électronique, toujours changeant et soumis à des évolutions constantes.

Bien entendu, ces cadres basés sur la catégorisation des informations en fonction du degré de sensibilité trouvent leur application dans de nombreux contextes. Ainsi, l'encadrement juridique de l'aire de partage proposée par P. Trudel trouve son fondement dans la classification des informations : « Pour délimiter ces aires de partage, il faut identifier des niveaux de protection différenciés qui devront trouver application en fonction du degré de sensibilité de l'information personnelle »[788]. Dans ce contexte, nous observons une catégorisation comportant les informations à caractère public, les informations des personnes échangées de façon anonyme, les informations nominatives et finalement, les informations relatives au cœur de la vie privée des personnes concernées.

Nous considérons que ces outils, utilisés en combinaison ou de façon unitaire, peuvent être d'une grande utilité dans le contexte des réseaux du secteur public. Ils témoignent de la complexité de décider dans ces environnements, comportant des particularités et des difficultés très spécifiques.
Nous analyserons, dans les pages qui suivent, comment le principe de finalité devient également un outil de protection essentiel dans les environnements en réseau et constitue un élément important du cadre de gouvernance à mettre en place afin d'assurer la protection de la vie privée des citoyens.

[788] P. TRUDEL, préc., note 12, 554.

## CHAPITRE 2 GOUVERNANCE DES RÉSEAUX, CIRCULATION DES INFORMATIONS ET RESPECT DE LA VIE PRIVÉE

Nous verrons dans ce dernier chapitre que le principe de finalité reste encore un des principes les plus importants dans le cadre de la gouvernance des réseaux. L'application de ce principe est tout à fait pertinent dans le contexte d'une gouvernance capable de protéger les renseignements personnels dans un environnement réseautique où les informations circulent de plus en plus. Dans le secteur public, la mise en place d'une véritable administration en réseau implique des échanges de renseignements personnels entre les différents organismes qui doivent être encadrés convenablement dans un contexte changeant en permanence.

La nature de « standard » pouvant caractériser le principe de finalité n'a fait que nous prouver que ce principe s'adapte de façon optimale aux changements pouvant s'opérer dans les réseaux. Toutefois, c'est grâce à de nouveaux standards reliés à ce principe de finalité que nous serons en mesure de créer un cadre de gouvernance vraiment adapté à un nouveau modèle d'administration. Nous analyserons les difficultés rencontrées pour arriver à déterminer ces nouveaux standards et les bénéfices retirés de leur utilisation afin de protéger les renseignements personnels utilisés et échangés dans le cadre des prestations électroniques de services.

De plus, nous observerons que la modélisation de certains processus d'évaluation des facteurs relatifs à la vie privée des programmes ou systèmes utilisant des renseignements personnels dans le secteur public peuvent aider à neutraliser les risques en la matière. Finalement, nous étudierons certains outils, que nous avons identifié comme les plus adéquats pour constituer un cadre de gouvernance efficace pour les structures en réseau. Ces outils, de natures différentes, utilisés de façon unitaire ou en les combinant avec d'autres, témoignent d'une certaine « adaptation réseautique » aux conditions prévalant dans ce type d'environnement.

Nous verrons également que le « droit en réseau » est le plus adéquat pour protéger les renseignements personnels dans les réseaux de l'administration. Il sera question, dans la dernière partie de ce chapitre, de comprendre dans quelle mesure ce droit « post-moderne » présente toutes les qualités pour garantir une véritable adaptation

réseautique : il est un droit pluriel, négocié, en évolution constante, produit en réseau, souple, flou, mou, transitoire et réflexif.

## SECTION 1 La pertinence du principe de finalité comme instrument de gouvernance des réseaux et l'importance des principes dans ce contexte

Suite à l'étude et à l'analyse de certains mécanismes pouvant servir *a priori* d'outils de gouvernance des structures en réseaux, il nous semble important de souligner le rôle que le principe de finalité peut être appelé à jouer dans ce contexte. En effet, l'adéquation des principes de protection des données personnelles en général, et plus particulièrement du principe de finalité, aux nouveaux modes de circulation de l'information est de plus en plus évidente.

La pertinence du principe de finalité est motivée par plusieurs facteurs, mais elle provient en partie de sa nature de « standard » qui rend possible d'une certaine façon une très juste adéquation aux nouveaux modèles de structure en réseau, et donc une circulation accrue des données.

### 1- Vers de nouveaux standards basés sur le critère de la finalité pour le modèle du réseau

Nous avons analysé dans les pages précédentes que le nouveau modèle en réseau qui s'impose actuellement, notamment dans le secteur public, présente des particularités ayant un impact sur les modes de circulation de l'information. De plus, nous avons constaté que le recours aux standards dans le droit, afin d'encadrer des nouvelles réalités, est devenu une pratique courante de la part du législateur et du juge.

Il nous semble que cette voie peut nous procurer des alternatives capables de fournir des solutions adaptées au contexte actuel. En effet, de nouveaux standards ayant leur point de départ dans l'idée se trouvant à l'origine du principe de finalité peuvent contribuer très clairement au développement de nouvelles formules aidant à la gouvernance.

Ainsi, certains concepts, tels que les « grappes de services », que nous avons pu identifier dans la littérature en la matière, témoignent de cette tendance. La problématique liée à la réutilisation des données à caractère personnel détenues par

les organismes appartenant au secteur public nécessite des concepts adaptés et adéquats afin de trouver des nouvelles voies d'encadrement.
Ces « grappes de services », concepts opérant dans le contexte du gouvernement électronique, témoignent de cet esprit visant à créer des groupes de données personnelles pouvant être utilisées dans le contexte de la prestation électronique des services.

Il nous semble que certains concepts, tels que les « familles de finalités »[789], peuvent aider à l'application du principe de finalité dans le contexte du réseau. Imaginons que l'utilisation de certains renseignements personnels dans le cadre d'une « famille de finalités » pourrait être encadrée, afin de protéger la confidentialité de telles données.
Ainsi, si nous sommes capables d'établir que certains renseignements personnels seront utilisés uniquement et exclusivement pour certaines finalités, nous pouvons garantir un degré de protection acceptable dans ce contexte. Ainsi, dans le cadre de l'État en réseau, « le respect du principe de finalité, suppose que l'usager ait effectivement connaissance des familles de finalités auxquelles serviront les informations au sein des réseaux de services publics »[790].

Si la protection est assurée, c'est à cause du fait que le rassemblement de ces finalités répond à une logique très claire, basée sur le principe de la compatibilité. Il s'agit alors d'une association ou rassemblement de finalités d'utilisation « compatibles ». Nous identifions ainsi, par exemple, un autre standard relié à ce principe, capable d'opérer dans une logique de réseau : « finalités compatibles ». Ces « familles de finalités », nouveau standard répondant à la logique des « finalités compatibles », mais également des « finalités adéquates » et des « finalités acceptables », que nous retrouvons dans les lois en la matière, constituent des nouveaux standards donnant réponse aux besoins identifiés dans le contexte de la mise en réseau de l'administration.

[789] P. TRUDEL, préc., note 754, 264.
[790] *Id*. (nous soulignons).

Il s'agit de concepts visant à limiter l'usage des renseignements personnels : « Pour respecter le principe de la limitation de l'utilisation, les environnements d'information devraient desservir des familles délimitées de prestations : ce qui assure que les renseignements personnels ne seront utilisés qu'à des fins apparentées et compatibles avec celles de la collecte initiale »[791].
Nous constatons ainsi que ces notions s'accordent parfaitement aux prestations électroniques de services devant être offertes aux citoyens.

Ces « familles de finalités » seront connues par les titulaires des données, ce qui va assurer une transparence garantissant la légitimité d'un tel procédé. Nous pouvons alors imaginer que, dans le contexte de l'administration électronique, le citoyen va savoir que certains de ses renseignements personnels seront utilisés et éventuellement échangés par des organismes du secteur public pour des utilisations très concrètes, liées par exemple au domaine de l'éducation et/ou du revenu. Dans d'autres cas, ce seront des utilisations de renseignements personnels reliées au contexte de la santé et de la sécurité sociale.
Mais, dans tous les cas et pour chaque prestation électronique de services, il sera important de déterminer si les utilisations et les finalités répondent à un critère de compatibilité et si la mise en commun de ces renseignements ne fait pas apparaître des risques en ce qui concerne la protection de la vie privée.
Pensons également aux réseaux mis en place dans le contexte de la recherche médicale et imaginons que les sujets ayant consenti à participer à une recherche puissent envisager que leurs renseignements médicaux et/ou génétiques vont pouvoir être échangés et utilisés par les différents centres de recherche faisant partie du réseau. Ces « familles de finalités » et d'autres nouveaux standards pouvant rendre compte du partage de données et de l'utilisation des renseignements pour différentes finalités peuvent être des outils d'une énorme importance dans ce contexte : des « grappes de finalités » ou des « finalités jumelées » peuvent exister parmi d'autres jouant un rôle important dans la gouvernance des réseaux.

[791] *Id*. (nous soulignons).

L'idée et l'esprit sont ceux qui se trouvent à l'origine du principe de finalité qui a vu le jour dans les premières législations en la matière et que nous avons analysé dans les pages précédentes. Toutefois, ces nouveaux standards, tels que celui de « famille de finalités » que le législateur n'a pas adopté et qui aujourd'hui ne se trouve pas dans le texte des lois, peuvent donner lieu à des moyens de protection adaptés aux nouvelles circonstances prévalant dans les environnements en réseau.
Ces nouveaux standards, pouvant être identifiés dans le but de protéger correctement les renseignements personnels dans le contexte des réseaux, se profilent comme des mécanismes dont les gestionnaires et les décideurs peuvent se servir afin de protéger convenablement les renseignements personnels.

Il nous semble que, après avoir compris le rôle majeur que les standards jouent déjà dans le droit relatif au droit d'auteur ou dans le droit relatif à la protection des renseignements personnels, il est nécessaire de comprendre l'importance d'un tel outil. Si l'application du principe de finalité dans ce contexte s'impose, c'est en partie à cause de sa nature de standard. Toutefois, pour que la pertinence d'un tel principe ne puisse faire l'objet d'aucun doute dans le contexte des réseaux, il nous semble important que des nouveaux standards reliés au principe de finalité et notamment adaptés à la circulation réseautique des renseignements personnels, viennent s'imposer comme des mécanismes indispensables à la gouvernance à mettre en place.

Si ces nouveaux standards sont basés sur l'idée préconisée par le principe de finalité, ils seront capables de donner une réponse face aux risques en matière de protection des informations à caractère personnel. De plus, ces concepts étant nouveaux et d'une nature ancrée spécialement dans les environnements en réseau et dans le contexte de l'offre des prestations électroniques de services, ils peuvent contribuer à l'application de ce principe de finalité, à partir d'une forme adaptée aux nouveaux environnements électroniques.

**2- Une certaine modélisation comme outil aidant à la gouvernance**

Nous pouvons déjà affirmer que les difficultés pouvant être identifiées dans la détermination de ces nouveaux standards seront nombreuses. Ce sont des difficultés prévalant dans le contexte de la protection des renseignements personnels dans les structures en réseau.

Prenons par exemple les questions entourant la détermination d'une « famille de finalités » : qui détermine quelles sont les finalités pouvant faire partie d'une même famille, quels sont les critères utilisés afin d'identifier une famille de finalités (compatibilité, adéquation, prévisions raisonnables de l'intéressé, etc.), comment et grâce à quel processus les familles de finalités sont-elles déterminées (décision des autorités de contrôle, consultation publique pour déterminer ces familles, processus démocratiques d'adoption de décision, adoption par comité d'experts, etc.), comment l'acceptabilité sociale de ces usages ou finalités des renseignements personnels est-elle assurée, etc.

Si ces exemples concernent spécialement le standard de « famille de finalités », ils existent également pour ce qui relève de la détermination du contenu de tous les nouveaux standards qui pourraient potentiellement opérer dans les environnements en réseau.

Et cela, parce qu'il est essentiel de réduire au maximum l'incertitude afin d'assurer un niveau adéquat de protection. Il est donc nécessaire de pouvoir compter sur une certaine « modélisation » de la décision capable de fournir un degré de prévisibilité aidant à assurer le niveau de certitude nécessaire aux processus décisionnels dans le contexte de la gouvernance des réseaux.

Cette modélisation peut donner lieu à une plus grande « tolérance » du risque en matière de respect du droit à la protection de la vie privée, puisque si nous établissons la modélisation de la décision devant servir *a posteriori*, mais

également de l'évaluation *a priori* des questions relatives à la protection des renseignements personnels dans les réseaux, nous allons pouvoir faire face aux dangers potentiels en matière de vie privée.

Grâce à l'analyse des décisions émanant des autorités de contrôle, nous pouvons de temps à autre identifier un certain manque de modélisation de ces décisions. Il est parfois difficile de comprendre quel est le *modus operandi* que les experts utilisent et complexe de saisir les étapes du raisonnement suivi, par exemple dans l'évaluation d'un programme comportant le traitement de données personnelles ou quand il s'agit de décider si des dispositions contenues dans les lois en la matière n'ont pas été respectées.

De plus, il est facile de percevoir aujourd'hui une certaine tendance à établir des « grilles » qui aident effectivement à structurer certaines démarches visant à déterminer le respect du droit relatif à la protection des renseignements personnels.
Ainsi, les ÉFVP au Canada, selon le modèle proposé par le Secrétariat du Conseil du Trésor dans sa directive de 2010[792] en la matière, propose un modèle d'évaluation structuré et prédéterminé.
La « ÉFVP de base », comportant des éléments standardisés de l'ÉFVP ayant un lien direct avec les obligations politiques et légales en matière de protection de la vie privée au Canada pour le secteur public, est un exemple de modélisation de l'évaluation. Ce nouveau modèle a permis d'améliorer les ÉFVP et à les perfectionner grâce à ce modèle comportant une grille de questions à considérer afin d'établir une évaluation complète et adaptée aux environnements du secteur public au Canada.
Il est question notamment de réussir, grâce aux différentes sections et informations présentes dans l'annexe contenant l'ÉFVP de base, de couvrir le contenu minimal d'une ÉFVP, en établissant un modèle unique.

[792] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 722.

Il nous semble intéressant de constater que certains proposent des procédures *ad hoc*, dans le contexte du gouvernement électronique et s'alignant sur la même tendance que celle des ÉFVP ou *Privacy Impact Assessment.*

K. Lenk, dans le cadre de ses travaux portant sur une « ingénierie administrative » visant à « faciliter le design des systèmes administratives dans le courant de la transformation administrative alimentée par les TIC »[793] et, notamment dans le cadre du gouvernement électronique, propose une procédure particulière.
En effet, il s'agit de l'*Innovation Impact Assessment*, procédure permettant d'évaluer *ex ante* la complexité de la mise en œuvre d'une politique publique et devant se réaliser au moment de la conception du projet en question.
Cette procédure, qui doit se réaliser en deux étapes, comporte notamment une première étape où il est nécessaire de discuter sur le système projeté en considérant principalement les « valeurs désirables » de la mise en place d'un tel projet, ainsi que les coûts-avantages. Les impacts potentiels sont évalués sur trois niveaux : individuel, organisationnel et sociétal. Lenk affirme qu'une « *awesome complexity* »[794] est créé au moment où s'accomplissent des démarches à suivre lors de cette première étape.

La deuxième étape induit un questionnement sur l'utilité d'introduire un tel système et oblige à l'analyse les raisons qui le justifient : opportunité, viabilité économique et sociale, etc.
Peu importe les étapes qui conforment ces procédures ou les points à analyser dans leur réalisation. Ce qui est essentiel, c'est que nous observons que des voix en Europe préconisent également la réalisation de ce type d'études qui répond à un modèle unitaire et prédéterminé et qui vise l'évaluation *a priori* de la pertinence des projets de gouvernement électronique.

---

[793] Klaus LENK, *Innovation Impact Assessment : une procédure pour évaluer ex ante la complexité de la mise en oeuvre d'une politique publique*, Présentation dans le cadre de l'Atelier Complexité et Politiques Publiques, tenu à Paris les 23 et 24 septembre 2010, en ligne : http://complexitejuridique.files.wordpress.com/2010/09/lenk_complex.ppt (consulté le 14 mai 2011).
[794] *Id.*

Les ÉFVP répondent également à cette même logique et leur réalisation est devenue une pratique courante depuis quelques années aux États-Unis et au Canada. Ces mécanismes paraissent offrir une « prédictibilité » qui devient de plus en plus nécessaire, ainsi qu'une certaine sécurité face à l'incertitude que caractérisent les nouveaux environnements électroniques aujourd'hui. La « modélisation » de ces procédures joue un rôle essentiel en ce qui concerne la pertinence de ces outils dans la gouvernance des structures réseautiques.

Parfois, cette modélisation passe par la création d'un « cadre analytique » important, pouvant donner comme résultat la structuration du débat entourant les questions de protection de la vie privée.
Plus particulièrement, nous pouvons affirmer que ce cadre analytique constitue un outil nécessaire pouvant servir à comprendre quelle est la démarche suivie par les décideurs. Ainsi, le CPVPC a publié en novembre 2010 un document ayant pour objectif de donner un « aperçu des étapes fondamentales et du cadre analytique utilisés par le Commissariat à la protection de la vie privée pour examiner des mesures législatives et des propositions des programmes, ou pour effectuer des examens de conformité par l'entremise des fonctions de vérification et d'enquête »[795].

Même si ce document s'inscrit spécifiquement dans une volonté d'intégrer le droit à la vie privée aux mesures de sécurité publique, il s'agit en définitive d'un document qui présente les détails relatifs aux « quatre étapes au cours desquelles il faut prendre en compte la protection de la vie privée »[796].

À notre avis, ces quatre étapes sont applicables non seulement aux questions relatives à la sécurité, mais également à toutes les questions concernant la protection de la vie privée et à toute démarche visant à déterminer si ce droit est

[795] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 634, p. 1.
[796] *Id.*

respecté dans le cadre de la mise en œuvre d'un programme ou d'une politique : la conception, la création, la mise en œuvre et l'examen.

Selon le CPVPC, certains facteurs, tels que les ÉFVP, doivent être pris en considération à chacune de ces quatre étapes dans le but de vérifier que la vie privée soit respectée et que tout fasse l'objet de documentation[797].

La première étape, relative à la conception, doit être orientée de manière à « établir le bien fondé », et cela en conformité avec la Charte canadienne des droits et libertés de 1982 et avec le critère de l'arrêt Oakes de la Cour suprême canadienne (nécessité, proportionnalité, efficacité et intrusion minimale), ce qui aidera à déterminer la pertinence de la collecte des renseignements en question[798].

La deuxième étape relative à la création est destinée à « définir les balises », ce qui induit l'examen des ÉFVP et des principes relatifs à l'équité dans le traitement des renseignements, tels que la détermination des fins de la collecte ou la limitation de l'utilisation, de la communication et de la conservation des renseignements personnels.

La troisième étape doit servir à « exécuter le programme », et cela grâce à l'intégration de la protection de la vie privée dans la gestion de l'information. Il s'agit, à cette étape, d'établir des mécanismes internes qui doivent être en réalité des moyens de maintenir le souci du respect du droit à la protection des renseignements personnels, tels que par exemple les ententes détaillées dans le contexte des cas d'échange de renseignements ou la présentation de forme régulière de rapports destinés au public et la publication de renseignements sur les ÉFVP.

Finalement, la quatrième étape est dévolue à « calibrer le système » moyennant des examens externes, ce qui s'explique parfaitement grâce à cette idée que le CPVPC expose : « en cette époque de réseaux d'échange de renseignements stratégiques, il nous faut des réseaux d'examen et de surveillance »[799]. Il s'agit, comme nous pouvons clairement le constater par la lecture de ce document émis par le CPVPC,

---

[797] *Id*,, p. 11.
[798] *R. c. Oakes, (1986) 1 S.C.R. 103*.
[799] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 634, p. 15 (nous soulignons).

de pouvoir compter dans ce contexte sur des « mécanismes de légitimité »[800]. Nous observons ici que le CPVPC n'hésite pas à affirmer qu'afin d'encadrer ces « réseaux » de surveillance de plus en plus puissants et performants, qu'il n'y a rien de mieux pour les encadrer que des « réseaux » capables de contrôler le fait que le droit à la protection de la vie privée est respecté. L'objet encadré et l'instrument capable d'établir sa bonne gouvernance, présentent tous deux une forme de réseau, afin de garantir la forme optimale du respect des droits fondamentaux en question, et cela à cause de la complexité et les caractéristiques propres aux réseaux où les informations circulent.

Ces quatre étapes que le CPVPC établit doivent servir à ce que la protection de la vie privée soit assurée à l'origine de tout programme ou projet et, même si le CPVPC parle de leur pertinence dans le contexte de la sécurité, il nous semble qu'elles s'appliquent parfaitement à toute circonstance mettant en cause la protection des renseignements personnels.
Il nous semble que ces étapes, établissant un « processus » fixe et prédéterminé, contribuent à offrir un « modèle » de démarche applicable à toute initiative pouvant avoir un impact en matière de vie privée.
L'établissement de ce modèle de démarche va aider sans doute les décideurs, les législateurs, les organisations ou administrations ainsi que les citoyens et tous les acteurs œuvrant dans le contexte de la mise en place de programmes ou d'initiatives, à ce que le droit fondamental à la vie privée soit respecté.

Grâce à cette modélisation du processus, un certain degré de sécurité et de confiance s'installe dans les rapports administration-citoyen, pouvant aider à une « bonne » gouvernance des réseaux. La possibilité de compter sur un cadre analytique capable d'assurer que tout programme et projet pouvant opérer dans les structures en réseaux sera respectueux du droit à la protection de la vie privée nous semble d'une grande nécessité à l'époque actuelle. De plus, d'une certaine façon,

[800] Pour avoir des informations plus précises sur les quatre étapes : *Id.*, p. 10 à 17.

cette « modélisation » aide en grande partie à la tolérance du risque et au choix des mesures visant à réduire un tel risque en matière de vie privée.

Plus concrètement, et comme exemple dans le cadre des opérations pouvant se développer dans les structures en réseau, nous pouvons imaginer la mise en place d'une prestation électronique de services opérée par une pluralité d'organismes publics.

Le partage de certaines informations entre les organismes et la mise en commun de quelques renseignements peut se révéler nécessaire afin d'offrir une prestation convenable au citoyen. Dans l'idée de la création de nouveaux standards capables de tenir compte de ce contexte, nous imaginons déjà que, par exemple les différents acteurs vont pouvoir identifier les finalités ou les usages pouvant faire partie de ces « familles de finalités » qui détermineront quels sont les renseignements qui seront utilisés dans le cadre de chaque prestation électronique de services.

Nous arriverons à réduire l'incertitude si le processus permettant d'identifier ces « familles de finalités » ou, par exemple, un autre nouveau standard comme celui des « finalités jumelées » répond à un modèle prédéterminé de processus.

Si les citoyens, les responsables au sein des organismes publics, les autorités de contrôle et le reste des acteurs dans le domaine peuvent avoir recours à un instrument capable de modéliser au maximum la décision, cela peut aider également à une plus grande tolérance du risque. Dans tous les cas, ces outils doivent pouvoir rendre compte des difficultés que présente le fait de décider dans des environnements complexes, caractérisés par des changements constants et parfois inattendus.

Toutefois, ces mécanismes et outils, ainsi que le cadre de gouvernance en général, doivent pouvoir s'adapter constamment aux nouvelles situations, toujours changeantes au sein des structures en réseau. En effet, le cadre de gouvernance doit pouvoir faire l'objet d'une certaine « adaptation réseautique » aux conditions prévalant dans les environnements en réseau.

### 3- Établissement et renforcement de certains principes en vue d'encadrer des structures en réseau : l'inter influence entre les principes

Nous assistons depuis un certains temps à une période de réflexion et de véritable demande de la part des experts et des autorités en la matière à propos de l'établissement d'un nouveau cadre de protection pour la protection des données. Au Canada et en Europe, la réforme des lois en vigueur est demandée depuis longtemps, et cela afin de créer un cadre plus adapté à la situation actuelle.
Si tous sont d'accord pour affirmer la pertinence des principes de protection présents dans les lois des deux côtés de l'Atlantique, certaines voix soulignent le besoin de leur application effective. De plus, le besoin de poser ou d'inclure certains principes dans la nouvelle régulation est affirmé également en vue d'inclure des obligations légales très concrètes. À notre avis, certains de ces principes devant être renforcés trouvent une application particulièrement adaptée aux environnements en réseau.

Il nous semble que l'influence mutuelle pouvant exister entre le principe de finalité et d'autres principes, comme celui de proportionnalité, ne fait que potentialiser les effets positifs de ces instruments dans la gouvernance des réseaux. Voici quelques principes présentant une grande pertinence dans le contexte actuel et qui vont sans doute pouvoir opérer en coordination avec le principe de finalité dans ce nouveau modèle gouvernance des réseaux.

#### A- Le principe de responsabilité

Depuis quelques années d'aucuns réclament l'établissement ainsi que le renforcement de certains principes en matière de protection des données personnelles. Les recommandations et les avis émanant des autorités, décideurs, groupes de réflexion et académiciens nous démontrent ce besoin et témoignent d'une certaine urgence dans l'accomplissement de telles réformes. En vue d'atteindre à un niveau plus élevé d'application effective des principes de

protection des renseignements personnels, des mécanismes complémentaires peuvent venir pour renforcer certaines obligations en la matière.

Nous allons essayer, dans les lignes qui suivent, d'analyser certains des principes qui, à notre avis, peuvent aider à renforcer l'application effective des règles de protection des données.

Ainsi, pour certains, il est nécessaire de pouvoir responsabiliser davantage les « responsables » du traitement. Le Groupe de l'article 29, notamment, n'a pas hésité à demander l'introduction du principe de « *accountability* » ou de responsabilité dans le régime de protection des données personnelles. En effet, le Groupe de l'article 29 voit « la responsabilité comme moteur de l'application efficace des principes de protection des données »[801] et formule une « proposition concrète en vue d'établir un principe de responsabilité exigeant des responsables du traitement des données qu'ils mettent en place des mesures appropriées et efficaces pour garantir le respect des principes et obligations définis dans la directive, et qu'ils le prouvent aux autorités de contrôle qui le demandent »[802].

Dans le contexte de la mise en place d'une administration en réseau et des services en ligne pour les citoyens, nous estimons d'une grande pertinence les réflexions de la Commission européenne sur l'importance du principe de responsabilité : « la simplification administrative ne devrait pas se traduire par une réduction générale du niveau de responsabilité des responsables du traitement à l'égard de la protection des données »[803].

Elle se positionne par rapport à ce débat en affirmant qu'elle étudiera les moyens de garantir que les responsables du traitement mettent en place des « politiques et mécanismes efficaces pour assurer le respect des règles en matière de protection

---

[801] GROUPE DE TRAVAIL « ARTICLE 29 », *Avis nº 3/2010 sur le principe de responsabilité*, adopté le 13 juillet 2010, p. 4.

[802] *Id.*, p. 2.

[803] COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS, préc., note 672, p. 13.

des données »[804] et affirme qu'elle tiendra compte du débat sur la possible introduction du principe de responsabilité dans la législation actuelle.

Le Groupe de l'article 29 avait déjà souligné l'importance du « renforcement de la responsabilité des responsables du traitement des données »[805] dans le contexte de la consultation de la Commission européenne sur le cadre juridique du droit à la protection des données personnelles.

Il faut noter que, dans le plan canadien et, plus concrètement, dans le cadre de la réforme de la LPRP, certains soulignent l'importance de renforcer le régime de responsabilité dans le contexte du secteur public au Canada : « une amélioration essentielle consisterait à modifier la Loi sur la protection des renseignements personnels de façon à demander la nomination de responsables de la protection des renseignements personnels (RPRP) au gouvernement du Canada et dans chaque institution gouvernementale, ou au moins dans celles qui font un usage important des renseignements personnels (qui recueillent, utilisent, communiquent et conservent de nombreux renseignements personnels sur des membres du public et sur des employés) »[806].

Le Groupe de l'article 29 a travaillé sur l'insertion du principe de responsabilité dans la version révisée de la directive et, plus concrètement, a étudié la question d'une « possible architecture juridique globale pour les mécanismes basés sur la responsabilité »[807]. Ainsi, cette architecture juridique prévoirait deux niveaux, le premier serait fondé sur une exigence légale fondamentale contraignante pour tous les responsables du traitement des données qui comprendrait deux éléments de fond : d'une part la mise en œuvre de mesures ou procédures et d'autre part la conservation d'une trace documentaire de celle-ci. Le second niveau « couvrirait des systèmes de responsabilité volontaires allant au-delà des exigences juridiques

[804] *Id.*
[805] GROUPE DE TRAVAIL « ARTICLE 29 » ET GROUPE DE TRAVAIL « POLICE ET JUSTICE », préc., note 761, p. 21.
[806] D. H. FLAHERTY, préc., note 262, p. 28.
[807] GROUPE DE TRAVAIL « ARTICLE 29 » , préc., note 801, p. 5.

minimales, eu égard aux principes sous-jacents de la protection des données (offrir des garanties supérieures à celles requises par les règles en vigueur) et/ou en termes de modalités de mise en œuvre ou de contrôle de l'efficacité des mesures (définir des exigences plus strictes) »[808].

Nous considérons que le principe de responsabilité peut constituer une excellente base pour les mécanismes servant à établir un cadre de gouvernance adapté au contexte actuel et devenir un outil indispensable dans la gestion des risques liés à la vie privée. Voici l'idée qui montre le besoin d'adoption d'une telle mesure dans le futur : « (...) il est absolument nécessaire pour les responsables du traitement des données de mettre en œuvre des mesures de protection des données efficaces, visant une bonne gouvernance en la matière, tout en réduisant au minimum les risques juridiques et économiques ainsi que les risques d'atteinte à la réputation susceptibles de résulter de mauvaises pratiques en matière de protection des données »[809].

L'adoption par le Groupe de l'article 29 d'un avis consacré uniquement à la question du principe de responsabilité démontre la grande importance que les obligations dérivées de l'adoption d'un nouveau régime de responsabilité auront dans l'avenir de la gouvernance dans les réseaux[810].

### B- Le principe de transparence et l'obligation de notification générale de violation de la vie privée

Dans le contexte de la circulation des renseignements personnels dans les structures en réseau, il nous semble que des mécanismes assurant la transparence peuvent devenir les outils les plus adaptés afin d'assurer une protection effective des données. La Commission européenne a identifié comme un des objectifs essentiels de l'approche globale de protection des données le fait d'accroître la transparence pour les personnes titulaires de données personnelles.

---

[808] *Id.*, p. 6.
[809] *Id.*, p. 5.
[810] *Id.*

Par conséquent, elle envisage d'introduire dans le cadre juridique un principe général de transparence pour le traitement des données[811]. En effet, pour la Commission, « il est donc primordial que les responsables du traitement informent les personnes concernées correctement et clairement, en toute transparence, afin qu'elles sachent qui recueillera et traitera leurs données, selon quelles modalités, pour quels motifs et pendant combien de temps, et qu'elles connaissent leurs droits en ce qui concerne l'accès à ces données, leur rectification ou leur suppression »[812].

Le Contrôleur européen souligne également l'importance du principe de transparence. Toutefois, il considère que ce principe fait déjà intégralement partie du cadre actuel de protection des données personnelles et, plus particulièrement, de la Directive 95/46/CE, même si c'est de façon implicite. Toutefois, pour le Contrôleur européen, le fait d'inclure explicitement ce principe de transparence dans le cadre de protection des données pourrait avoir un effet bénéfique, même s'il considère comme crucial le fait de renforcer les dispositions déjà existantes en matière de transparence.

Bien entendu, la transparence est un outil absolument nécessaire à la gouvernance des structures en réseau, afin que le titulaire puisse retrouver le contrôle de la gestion des renseignements le concernant. De plus, la transparence est un élément essentiel pour la gestion des fuites ou du vol des données. Ainsi, la Commission européenne s'est engagée à étudier la question de l'introduction, dans le cadre juridique de protection des données personnelles en Europe, d'une « obligation générale de notification des violations de données à caractère personnelle, indiquant les destinataires de ce type de notifications et les critères auxquels serait subordonnée l'application de ce obligation »[813].
Pour certains, une des mesures de nature « réactive » à adopter en matière de protection des données serait l'obligation de notification en cas de violation de la

[811] COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS, préc., note 672, p. 6 et 7.
[812] *Id.*, p. 6.
[813] *Id*,, p. 8.

sécurité des données[814]. Le Contrôleur européen, qui appuie la position de la Commission européenne, encourage également l'adoption de cette obligation et souligne l'importance du rôle qu'une telle obligation peut avoir afin que les personnes concernées soient préparées face au risque dérivant de la violation des données ou *data breach*[815].
Certains auteurs américains encouragent également l'adoption de cette obligation de notification en vue de minimiser les risques rendant plus vulnérables les personnes concernées, tels que la fraude et le vol d'identité[816].

Bien sûr, cette obligation de notification peut avoir d'autres bénéfices, le Contrôleur européen avance d'ailleurs à ce sujet :

> « *In addition, security breach notification contributes to the effective application of other principles and obligations in the Directive. For example, security breach notification requirements incentivize data controllers to implement stronger security measures to prevent breaches. Security breach is atool to strengthen the responsability of data controllers and, more in particular to enhance accountability.* »[817]

En effet, la question relative à l'obligation de sécurité des systèmes d'information peut se voir renforcée grâce à l'adoption de l'obligation de notification de violation. En tout cas, il nous semble que cette obligation de notification est très clairement devenue une des manifestations les plus importantes du principe général de transparence et un outil vraiment adéquat pour une bonne gouvernance des structures en réseau. De plus, il est un des meilleurs instruments pour créer un sentiment de confiance envers les programmes ou prestations dans le cadre de projets tels que l'administration électronique dans les réseaux du secteur public.

---

[814] GROUPE DE TRAVAIL « ARTICLE 29 » ET GROUPE DE TRAVAIL « POLICE ET JUSTICE », préc., note 761, p. 24.
[815] CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, préc., note 675, p. 17.
[816] Voir à ce sujet : Daniel J. SOLOVE et Chris Jay HOOFNAGLE, « A Model Regime of Privacy protection Version 2.0 », *GWU Law School Public Law Research Paper*, n° 132, avril 2005.
[817] CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, préc., note 675, p. 17.

### C- Principe de nécessité des données

Finalement, nous observons que pour certains le principe de nécessité peut représenter un mécanisme d'une grande utilité dans le contexte de la protection des données personnelles dans les réseaux de l'administration.

Le CPVPC affirme que, pour que le gouvernement fédéral canadien recueille le moins d'informations possible, il encourage l'introduction dans la LPRP du caractère obligatoire d'un « test de nécessité », en forçant les organismes à prouver la vraie nécessité de leur action à l'heure de collecter des renseignements[818].

Dans un contexte européen, certains évoquent un « principe de minimisation » qui prescrirait de réduire au maximum la collecte des informations à caractère personnel[819]. Voici comment ce principe est envisagé dans le cadre de l'administration électronique :

> « Si une commune souhaite accorder des réductions de taxe communales à certains citoyens au revenu modeste, point n'est besoin de fournir les revenus précis des citoyens bénéficiaires. Une simple liste des personnes, sans mention du niveau exact du revenu, suffit. »[820]

La Commission européenne s'est engagée à étudier, dans le contexte du nouveau cadre européen sur la protection des données, le renforcement du « principe de la minimisation des données », qu'elle associe à l'idée que « le traitement des données par les responsables doit être limité à des finalités bien précises »[821].

---

[818] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, préc., note 531, p. 10.
[819] David DE ROY, Cécile DE TEWARGNE et Yves POULLET, *La Convention européenne des droits de l'homme en filigrane de l'administration électronique*, version mise à jour d'une présentation orale au colloque sur « Cinquante ans d'application de la CEDH en Belgique : entre ombres et lumières », organisé par le Centre de recherche en droit public de l'ULB, les 20 et 21 octobre 2005 à Bruxelles, p. 340, en ligne : http://www.crid.be (consulté le 3 avril 2011).
[820] *Id.*
[821] COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS, préc., note 672, p. 8.

Ce principe peut réellement aider à minimiser les risques liés à la protection de la vie privée, puisqu'en minimisant le nombre de données faisant l'objet d'un traitement ainsi que les différentes opérations sur l'information, les problèmes peuvent diminuer considérablement.
De plus, si on associe l'idée de minimisation et celle de finalité, nous pouvons en effet, arriver à réduire le risque d'utilisations non autorisées des informations dans un réseau.

Dans un contexte de généralisation des réseaux, certains soulignent l'importance du fait que, dans le cadre d'un processus décisionnel spécifique, les seules informations qui font l'objet d'une utilisation sont celles qui se révèlent vraiment pertinentes et autorisées. Pour y arriver : « Cela appelle une démarche dans laquelle sont dissociées, d'une part, la question de la nécessité de la détention de l'information et, d'autre part, l'appréciation de la nécessité d'y accéder pour une décision ou prestation déterminée »[822].

En conséquence, dans un contexte réseautique, ce principe de nécessité doit encadrer la détention, les accès, l'utilisation et bien d'autres opérations concernant les informations, si on veut être sûr de protéger la confidentialité pendant tout le cycle de vie des informations.
Les solutions techniques peuvent jouer un rôle majeur dans le respect du principe visant à minimiser les renseignements personnels circulant dans les réseaux, surtout si elles accompagnent depuis le début la mise en place de programmes et de projets opérant dans le secteur public.

[822] P. TRUDEL, préc., note 754, 264 (nous soulignons).

## SECTION 2 Adaptation réseautique des systèmes de protection des renseignements personnels aux conditions prévalant dans les environnements en réseau

Nous observons comment un cadre destiné à la gouvernance des structures en réseau peut être défini, et cela grâce à des outils de natures très différentes. Ce cadre doit être capable de protéger les renseignements personnels dans le contexte de ces structures et nécessite une exceptionnelle capacité d'adaptation permanente, que nous avons voulu qualifier de « réseautique », à l'image même de l'objet encadré.

Le principe de finalité, qui se trouve au centre de ce cadre, et les différents outils et mécanismes aidant à son application et devant être capables d'opérer au sein d'un système de gouvernance cohérent doivent répondre à un modèle d'adaptation continuelle et dynamique.

Le système de protection du droit à la vie privée opérant dans les structures en réseau, va devoir être encadré du point de vue théorique par une conception du droit qui va nous permettre d'appréhender clairement les enjeux de l'application du principe classique de finalité à l'égard de la protection des renseignements personnels dans ce contexte.

Ce système de protection des renseignements personnels, ce cadre de gouvernance ou, plus généralement, ce droit que nous pouvons qualifier de *post-moderne*, se présente comme un droit non hiérarchique, linéaire, en forme de réseau, pluriel, négocié, souple, flou, mou, transitoire, réflexif et qui est également formé où élaboré en réseau.

Cette approche théorique va nous permettre de bien comprendre le processus d'adaptation réseautique du droit relatif à la protection des renseignements personnels au nouveau modèle de circulation des informations à caractère personnel au sein de l'administration et du secteur public en général.

Il faut souligner que nous avons voulu approfondir également dans l'étude concret des fondements du principe de finalité et cela, afin d'être en mesure d'identifier quels peuvent être les moyens de nature normative, mais aussi de nature technique,

à mettre en place afin de garantir l'application effective de ce principe dans l'environnement en réseau de l'administration.

Par ailleurs, nous avons vérifié, dans nos travaux, l'existence d'une idée assez répandue aujourd'hui, tant au Canada que dans le contexte européen, préconisant le besoin d'adaptation des régulations relatives à la protection des renseignements personnels à une nouvelle réalité. Le principe de finalité nous aide à véhiculer nos propos quant à la métamorphose que nous observons dans la structure et la dynamique de fonctionnement des espaces de circulation des informations.

Nous observons que, parfois, le droit relatif à la protection des renseignements personnels est devenu « rigide » devant la dynamique qui caractérise les espaces où les informations circulent. Sans doute, le principe de finalité, parmi les principes de protection des renseignements personnels, est en mesure de symboliser mieux que n'importe quel autre la capacité d'adaptation de la législation en vigueur.

Certains auteurs ont fait remarquer que nous assistons depuis quelques années à une « rigidification » du principe de finalité, ce qui a pour résultat l'immobilisation de l'information personnelle[823]. Nous pouvons imaginer la notion « fixe » et rigide de ce principe et nous constatons que cette représentation s'ajuste difficilement au modèle du réseau.

Toutefois, nous avons pu constater que la nature de ce principe, pouvant opérer en tant que « standard » juridique, nous indique la voie pour réfléchir à une vision plutôt « réseautique » du principe de finalité notamment, et des systèmes de protection des renseignements personnels en général. Il est évident pour nous que ce principe ainsi que les autres principes de protection des données personnelles restent de toute actualité et symbolisent, plus que jamais, l'importance des systèmes basés sur certaines règles et principes applicables à des environnements toujours changeants et évolutifs.

Il nous semble que nous devons essayer d'envisager ce nouveau modèle de système de protection en vertu du cadre théorique relatif à un droit qui ne présente plus les caractéristiques propres du droit classique hiérarchique[824] et en forme de pyramide,

[823] P. TRUDEL, préc., note 148, p. 13.
[824] Bruno OPPETIT, *Droit et modernité*, Paris, P.U.F., 1998, p. 7.

mais qui présente une certaine forme de réseau, non seulement en ce qui concerne sa structure, mais aussi dans la forme que prend son processus de création.

En outre, comme certains auteurs l'ont souligné, les principes directeurs vont permettre au droit d'accroître sa complexité en fournissant les liens permettant la mise en rapport de normes très diverses[825]. Ces principes sont « garants d'une interlégalité horizontale entre plusieurs législations finalisées »[826]. Nous pouvons donc constater que le principe de finalité, qui est un principe directeur en matière de protection des renseignements personnels, devient un outil indispensable dans l'étude de la manière dont les différents instruments encadrant la circulation des informations doivent se formuler de façon à être adaptés au nouveau modèle de réseau.

Nous analyserons dans les pages qui suivent, quelles sont les particularités du droit que certains auteurs ont qualifié de droit post-moderne, afin de montrer que cette conception est la plus adaptée au cadre de gouvernance devant opérer dans les environnements en réseau. Il sera question également d'analyser les caractéristiques du « droit en réseau », capable d'offrir un cadre de gouvernance adéquat aux structures actuelles appartenant au secteur public et susceptible d'offrir les outils les plus adaptés aux structures en réseau. Les « normativités en réseau » deviennent effectivement des modèles d'adaptation maximale, très sensibles à l'évolution permanente des structures permettant la circulation accrue des informations.

**1- Un « droit en réseau » pour encadrer le réseau**

Nos travaux ont été très fortement influencés par une notion centrale qui a toujours existé, mais qui occupe une place de plus en plus importante suite à l'utilisation massive des technologies de l'information et de la communication au sein de nos

[825] C.-A. MORAND, préc., note 19, p. 190.
[826] *Id.*

sociétés. Ce concept est celui du « réseau », qui constitue pour certains la « caractéristique majeure de la société de l'information »[827].

M. Castells travaille sur la théorie des réseaux depuis des années et sur le concept de réseau, qu'il définit comme « un ensemble de nœuds interconnectés »[828]. Il ajoute qu'un nœud est un point d'intersection d'une courbe par elle même et que « la réalité d'un nœud dépend du type de réseau auquel il appartient »[829].

Ainsi, « le réseau repose sur une analogie, celle du "filet", dont la figure offre une illustration des liens normatifs qui se tissent entre des acteurs multiples souvent inégaux et des situations diverses survenant dans une pluralité de juridictions »[830].

Pour K. Benyekhlef, « le réseau se caractérise par sa mobilité, sa plasticité et son ouverture »[831].

P. Trudel voit les réseaux comme des « environnements interconnectés et organisés dans lequel l'information circule d'un pôle à l'autre, de façon multidirectionnelle et non-hiérarchique »[832].

C'est important de constater le fonctionnement spécifique de ces réseaux aujourd'hui : « l'inclusion/exclusion dans les réseaux et l'architecture des relations entre les réseaux, mises en œuvre au moyen de technologies opérant à la vitesse de la lumière, dessinent les fonctions et les processus dominants dans nos sociétés »[833]. Nous constatons chaque jour qu'en effet, cette nouvelle réalité s'impose à tous les niveaux de la société et dans tous les domaines

Pour M. Castells, « les réseaux sont des structures ouvertes, susceptibles de s'étendre à l'infini, intégrant des nœuds nouveaux en tant qu'ils sont capables de communiquer au sein du réseau, autrement dit qui partagent les mêmes codes de communication »[834]. De plus, cet auteur identifie certains éléments du « paradigme de la technologie de l'information », qui, ensemble, vont composer la « base

---

[827] Manuel CASTELLS, *La société en réseaux, L'ère de l'information*, Paris, Fayard, 2001, p. 576.
[828] *Id.*
[829] *Id.*
[830] Karim BENYEKHLEF, *Une possible histoire sur la norme*, Montréal, Éditions Thémis, 2008, p. 716.
[831] *Id.*.
[832] P. TRUDEL, préc., note 12, p. 533.
[833] M. CASTELLS, préc., note 827, p. 576.
[834] *Id.*

matérielle de la société en réseaux »[835]. La « souplesse », liée à l'intégration en réseau, est intiment liée à l'essence même de ce nouveau paradigme :

> « Ce qui caractérise la configuration du nouveau paradigme technologique, c'est sa capacité de réorganisation, aspect essentiel dans une société marquée par le changement constant et la fluidité organisationnelle. Inverser les règles sans détruire l'organisation est devenu possible, parce que la base matérielle de l'organisation peut être reprogrammée et structurée. » [836]

Cette souplesse va sans doute contribuer à trouver un cadre de gouvernance pertinent et adapté à des phénomènes toujours changeants et évolutifs. Dans le contexte de nos travaux, nous parlons des structures en réseau au sein de l'administration, des architectures réseautiques caractérisant aujourd'hui le secteur public et, plus concrètement, d'un « État en réseau » caractérisé par l'utilisation généralisée des technologies.

Le droit capable d'encadrer un tel phénomène est également un « droit en réseau », une « normativité en réseaux ». Nous constatons alors que « la présence, dans un réseau, d'une pluralité d'acteurs aux statuts divers et aux rapports de force variables multiplie les foyers d'autorité et de normativité »[837].

Cette « normativité en réseaux » est inhérente aux structures en réseaux, que ce soit dans le contexte de la cybersanté[838], du cybergouvernement mais également du cyberespace[839] en général et d'Internet. Voici comment cette normativité en réseaux se dessine, à partir de l'objet même qu'elle encadre :

> « L'espace auquel on a affaire est un ensemble interconnecté constitué de pôles interagissants de normativités. Il est constitué d'espaces dans lesquels prévalent en tout ou en partie des normes qui s'imposent aux usagers. Cet espace est aussi constitué de relais par lesquels s'explicitent et se diffusent les normativités et les conséquences de

[835] *Id.*, p. 100.
[836] *Id.*, p. 102 (nous soulignons).
[837] K. BENYEKHLEF, préc., note 830, p. 726.
[838] Pierre TRUDEL, « Gouvernance réseautique et effectivité des modes de protection des données personnelles dans les réseaux de cybersanté » dans Jean HERVEG (dir.), *La protection des données médicales, Les défis du XXI^e siècle*, dans, Louvain-la-Neuve, Anthémis, 37.
[839] P. TRUDEL, préc., note 717.

> celles-ci. Les règles émanant des pôles de normativité se relayent et se diffusent dans les différents espaces virtuels. Elles coexistent soit en complémentarité avec d'autres règles, soit en concurrence, se proposant à la place de celles qui sont issues d'autres pôles normatifs. »[840]

Il s'agit effectivement d'une normativité constituée de « nœuds » de normativité, tels que les normes, les pratiques du réseau ou la normativité découlant de la technique, mais également de « relais » de normativité qui sont les différents moyens par lesquels les acteurs d'un environnement en réseau vont recevoir et appliquer effectivement les normes qu'ils considèrent comme « importantes » ou « obligatoires »[841].

Pour P. Trudel, ces relais sont nécessaires afin d'assurer les « arrimages » entre les différentes normativités et il en cite quelques-uns, tels que les régimes de responsabilité, mais également l'autorégulation et la corégulation, principaux relais encadrant les activités qui se déroulent dans le cyberespace.

De plus, ces nœuds et relais de normativité « sont en lien d'intrerinfluence »[842], ce qui à notre avis, témoigne de la capacité d'adaptation réseautique propre à cette normativité.

Il nous semble que le nouveau cadre de protection des renseignements personnels, capable d'encadrer les flux d'information dans les réseaux, réaffirmera ce modèle de normativité et intégrera les mécanismes dont nous avons parlé dans les pages précédentes, qui ne pourront pas échapper à ce lien d'interinfluence.

**2- Un droit « post-moderne » pour une adaptation réseautique**

Nous analyserons dans les pages qui suivent les caractéristiques de cette « normativité en réseau », présentant les éléments d'un « droit post-moderne » que nous tenterons d'identifier.

---

[840] P. TRUDEL, préc., note 838, 39 (nous soulignons).
[841] Voir à cet effet : P. TRUDEL, préc., note 838, 39 et s.
[842] Voir sur cette définition : P. TRUDEL, préc., note 717.

Dans un texte de 1998, J. Chevallier a émis l'hypothèse de « l'avènement dans les sociétés contemporaines d'un droit nouveau, un droit post-moderne, qui serait radicalement différent du droit classique et donnerait à la régulation juridique une portée singulière »[843].

Certains auteurs parlent d'un changement de paradigme : de la crise du modèle pyramidal émerge un paradigme concurrent, celui du « droit en réseau », dans lequel nous reconnaissons les caractéristiques de ce droit post-moderne que J. Chevallier a mentionné. Pour certains, « le paradigme dominant du droit, la pyramide, disparaît au profit du réseau »[844].

F.Ost et M. Van de Kerchove décrivent ce droit en réseau :

> « Avec le réseau, l'État cesse d'être le foyer unique de la souveraineté (celle-ci ne se déploie pas seulement à d'autres échelles, entre pouvoirs publics infra et supra étatiques, elle se redistribue également entre de puissants pouvoirs privés) ; la volonté du législateur cesse d'être reçue comme un dogme (on ne l'admet plus que sous conditions, au terme de procédures complexes d'évaluation tant en amont qu'en aval de l'édiction de la loi) ; les frontières du fait et du droit se brouillent ; les pouvoirs interagissent (les juges deviennent co-auteurs de la loi et les subdélégations du pouvoir normatif, en principe interdites, se multiplient) ; les systèmes juridiques (et, plus largement, les systèmes normatifs) s'enchevêtrent ; la connaissance du droit qui revendiquait hier sa pureté méthodologique (mono-disciplinarité) se décline aujourd'hui sur le mode interdisciplinaire et résulte plus de l'expérience contextualisée (learning process) que d'axiomes a priori ; la justice, enfin, que le modèle pyramidal entendait ramener aux hiérarchies de valeurs fixées dans les lois, s'appréhende aujourd'hui en termes de balances d'intérêt et d'équilibration de valeurs aussi diverses que variables. »[845]

Nous tenterons de montrer que le « droit en réseau » présente des caractéristiques équivalentes à celles du droit post-moderne dont J. Chevallier fait mention. Pourtant, il ne faut pas oublier que, au sein de ce droit en réseau, des « résidus» importants du droit en pyramide sont restés, ce qui va complexifier encore plus ce

---

[843] JACQUES CHEVALLIER, « Vers un droit post-moderne ?», *R.D.P.*, nº 3-1998, 660.
[844] K. BENYEKHLEF, préc., note 830, p. 717.
[845] François OST et Michel Van de KERCHOVE, *De la pyramide au réseau ?*, Bruxelles, Publications des Facultés universitaires Saint-Louis, 2002, p. 14. (nous soulignons).

phénomène. Pour certains, la « cohabitation » des traits du droit moderne et du droit post-moderne, et même leur assemblage, devient nécessaire aujourd'hui :

> « (...) Le droit dit postmoderne n'échapperait pas à cette condition : le contexte contemporain nous oblige à réviser les fondements « modernes » du droit afin de lui rendre ses qualités normatives opérantes. Ce contexte nous contraint à rompre, parfois radicalement, avec certains postulats de la dogmatique juridique, mais cette rupture ne signifie pas, encore une fois, qu'il faille faire *tabula rasa* de tous les traits du droit moderne. Un croisement, un métissage un mélange doivent être accompli afin de trouver l'heureux équilibre d'un droit susceptible de saisir le présent. La tâche est importante. »[846]

En effet, c'est l'objectif du droit post-moderne que d'être capable d'encadrer la réalité actuelle en dépassant les limites du droit moderne, telles que certains « postulats de la dogmatique juridique qui l'empêchent de refléter adéquatement les réalités contemporaines et d'accomplir son office essentiel : offrir un cadre normatif aux rapports globaux qui se nouent parmi les nouveaux acteurs de la globalisation et proposer des solutions concrètes et effectives aux nouveaux défis des interdépendances et de la gestion globale des risques »[847]. C'est sans doute, un défi difficile à réussir, en partie à cause des « situations globales de menace » qui existent aujourd'hui, par opposition aux « risques personnels »[848] qui existaient par le passé et que le droit moderne arrivait à neutraliser sans problèmes majeurs.

Nous considérons que ce cadre théorique, qui envisage le droit en réseau, est celui qui va réellement pouvoir nous aider dans le contexte de nos recherches portant sur l'application du principe de finalité comme principe recteur en matière de protection des renseignements personnels dans le contexte des environnements en réseau.

C.-A. Morand nous rappelle, d'une part, l'importance de l'homologie entre la structure sociale et la structure juridique, qui présentent toutes deux la forme d'un réseau et, d'autre part, l'importance du paradigme réseautique :

---

[846] K. BENYEKHLEF, préc., note 830, p. 558 (nous soulignons).
[847] *Id*.
[848] Ulrich BECK, *La société du risque, Sur la voie d'une autre modernité*, Paris, Aubier, 2001, p. 39. Cet auteur met en opposition le concept existant dans le passé du « risque personnel » face aux « situations globales de menace » que nous connaissons aujourd'hui.

> « […] Celui-ci (le paradigme du réseau) permet de rompre délibérément avec le modèle mécanique, linéaire et hiérarchique du droit moderne. Il donne la possibilité au droit de s'adapter à la structure sociale. Or, il ne fait pas de doute que les réseaux constituent la nouvelle morphologie sociale de nos sociétés. C'est en prenant conscience de la très large homologie entre la structure sociale et la structure juridique qu'il sera possible d'éviter les simplifications déformantes, que l'on pourra faire en sorte que les pratiques judiciaires ou les dispositions de procédure ne réduisent pas à néant la complexité établie par le droit de fond. »[849]

En effet, nous observons qu'une très forte homologie peut être identifiée entre la structure des environnements numériques et la structure juridique qui est essentiellement réseautique.

Nous sommes en mesure d'utiliser le terme « adaptation réseautique » afin d'exprimer les particularités des processus accompagnant la formation du cadre de protection de la vie privée dans les réseaux. Nous constatons que si nous concevons le droit sous cet angle, il devient alors pensable d'envisager une possible adaptation du droit relatif à la protection des renseignements personnels à la nouvelle réalité sociale représentée dans le cadre du secteur public par le réseau de l'administration électronique.

Nous assistons depuis quelques années, à la naissance et à la formation d'un droit nouveau, propre à l'État post-moderne, qui présente des caractéristiques que, selon certains auteurs, le droit n'a jamais connu auparavant.

Afin de savoir comment est constitué ce droit post-moderne dont certains parlent, il faut premièrement chercher une définition de ce qu'est le droit moderne. B. Oppetit explique à ce sujet :

> « Loin d'être le droit voulu par les individus libres au sein d'une société contractuelle, le droit moderne apparaît bien plutôt, pour l'essentiel, comme un droit hiérarchique, généré par une phénomène de pouvoir et élaboré par une technocratie politique, administrative et économique et légitimé par des doctrines positivistes, normativistes

[849] C.-A. MORAND, préc., note 19, p. 207 (nous soulignons).

> ou décisionnistes. Le droit moderne appartient pour l'essentiel à un ordre légaliste, édictant des interdictions et des prescriptions ; or, le discours proprement juridique n'est pas déontique : il se borne à dire ce qui revient à chacun et à définir des procédures sans se soucier des résultats auxquels elles mènent. Le droit moderne, tout au contraire est un droit de solutions, préoccupé du contenu matériel des règles. »[850]

En ce moment, la question que nous devons nous poser est celle de savoir en quoi consiste ce droit post-moderne ? Et par conséquent, quelles sont ses caractéristiques nouvelles par rapport au droit moderne et au droit en pyramide ?

K. Benyekhlef a affirmé en 2008 que le droit postmoderne était encore une « esquisse » et qu'il restait encore beaucoup à ébaucher dans la matière, affirmation que nous partageons en 2011. Cependant, cet auteur est capable de nous expliquer en très peu de mots la capacité de ce droit à répondre aux nouveaux défis posés par une nouvelle réalité : « à la simplicité de la modernité, répond la complexité de la postmodernité, son rejet des oppositions duales au profit d'une dialectique qui en opère la synthèse et le remplacement progressif du paradigme de la pyramide, caractéristique du droit moderne, par celui du réseau beaucoup plus approprié aux réalités contemporaines »[851].

Nous essayerons également de comprendre pourquoi ce droit fait figure de théorie adéquate pour encadrer les travaux de recherche en droit des technologies de l'information et, particulièrement, en droit relatif à la protection des renseignements personnels.

Finalement, nous allons être en mesure de justifier le choix de ce cadre théorique afin d'étudier les fondements du principe de finalité et, ainsi, arriver à comprendre comment ce principe va devoir être appliqué dans les environnements en réseau.

### A- Un droit pluriel

Ce droit est un droit « pluriel » et nous pouvons constater que la conception moniste du droit moderne s'est vue remplacée par une vision pluraliste à cause de la multiplication des divers foyers de droit. La thèse du pluralisme juridique est

[850] B. OPPETIT, préc., note 824, p. 7.
[851] K. BENYEKHLEF, préc., note 830, p. 557.

essentielle pour comprendre le scénario juridique actuel. Nous le savons, nous pouvons identifier une multitude de théories sur le pluralisme juridique. Pourtant, N. Rouland affirme que « toutes les théories du pluralisme juridique ont en commun de relativiser la place de l'État par rapport à la société, et d'affirmer qu'il existe des droits non-étatiques engendrés par les groupes sociaux constitutifs de toute société »[852].

En effet, l'État cède sa place de créateur exclusif du droit et d'autres acteurs contribuent à élargir le champ du juridique. J. Chevallier a signalé en 1983, dans un de ses articles, la perte d'exclusivité de l'ordre juridique étatique :

> « Malgré ses prétentions totalisantes et sa recherche de l'exclusivité, l'ordre juridique étatique ne parvient jamais à ramener à lui et à condenser la totalité des phénomènes juridiques et il se trouve pris à revers et court-circuité par des règles juridiques qui se forment en des multiples lieux et échappent au moins partiellement à sa médiation. »[853]

Ce même auteur signale également que « […] l'État n'apparaît plus que comme un producteur de droit parmi d'autres ; l'ordre juridique étatique est pris en tenaille entre des ordres juridiques infra-étatiques, fondés sur des solidarités "partielles" ou "locales" , et des ordres juridiques supra-étatiques, nés de l'émergence de communautés plus larges, "régionales" (par exemple, l'ordre juridique européen) ou "mondiale" (ordre juridique international) "mondialisation juridique" répondant à la "mondialisation économique »[854].

Ce phénomène est sans doute lié à la notion même de « souveraineté », que certains auteurs considèrent « en mutation »[855], notion qui exerce une influence importante sur le rôle traditionnel de l'État en tant que seul et unique créateur du droit ainsi

---

[852] Norbert ROULAND, « Anthropologie juridique », dans D*roit politique et théorique*, Paris, P.U.F., 1988, p. 26.
[853] Jacques CHEVALLIER, « L'ordre juridique », dans *Le Droit en procès*, Paris, P.U.F., 1983, p. 43.
[854] J.CHEVALLIER, préc., note 843, 673.
[855] K. BENYEKHLEF, préc., note 830, p. 559 et s.

que sur la création de nouveaux ordres juridiques n'appartenant pas à l'ordre national ni à l'ordre international[856].

Nous pouvons voir que cette multiplication des acteurs créateurs du droit touche aux différentes disciplines et devient la règle générale dans les différents systèmes juridiques du monde. Cependant, nous ne pouvons pas nier que, ces dernières années, le droit relatif aux nouvelles technologies de la communication et de l'information constitue un bon exemple de droit « pluriel ». Les raisons expliquant ce phénomène sont de natures très diverses, nous allons le voir dans les pages qui suivent. En réalité, nous ne pouvons pas concevoir ce droit relatif à Internet et aux différents phénomènes reliés au réseau comme un droit exclusivement étatique :

> « Prenons le cas du droit et des changements technologiques. Voici un ensemble de problèmes où des changements extrêmement rapides dans les sciences et les techniques (l'informatisation, par exemple, ou encore le génie génétique ou les connaissances scientifiques sur l'énergie) posent au droit une série de problèmes nouveaux et souvent urgents. Ces problèmes se ramènent tous à préciser quel type de régulation (législation, règlements, contrats, etc.) et quelles normes peuvent le mieux contrôler ces développements, protéger les individus, l'environnement, sans nuire par ailleurs au progrès scientifique et technologique. »[857]

J. Chevallier nous présente l'exemple de la régulation d'Internet, qui s'avère possible grâce à la participation de plusieurs acteurs, mais qui va supposer aussi une caution étatique, ce qui nous permet de parler du phénomène de l'autorégulation[858]. Le réseau Internet est aussi un reflet de la société, il est pluriel, hétérogène, multiple et mondial ou mondialisé. Ce réseau implique la participation dans sa régulation de plusieurs acteurs (utilisateurs, groupes actifs dans le réseau, associations et groupes de pression, etc.), mais Internet n'échappe pas aux États.

---

[856] *Id.*, p. 671.
L'auteur nous rappelle que le droit communautaire européen forme un nouvel ordre juridique distinct qui a comme des sujets de droit les États, mais également les personnes physiques ou morales.

[857] Guy ROCHER, « Pour une sociologie des ordres juridiques », *Les Cahiers de Droit*, vol. 29, nº 1, mars 1988, 116.

[858] J. CHEVALLIER, préc., note 10, p.113 et 114.

De plus, l'environnement en réseau aura des conséquences sur la manière de concevoir la légitimité de l'intervention de l'État :

> « L'espace résultant de l'environnement-réseau présente des balises définissant différemment de celles de l'espace physique. En favorisant une redéfinition des espaces de référence, la virtualisation porte le germe d'une mutation des paramètres selon lesquels se conçoit la légitimité des interventions étatiques. »[859]

Dans le cadre de nos recherches, quand nous parlons de moyens « normatifs » et des « mécanismes » pour garantir l'effectivité à l'heure d'appliquer le principe de finalité à l'égard de la protection des renseignements personnels dans le contexte de l'État en réseau, c'est pour laisser la porte ouverte à un éventail d'instruments de natures très différentes, comme ceux que nous avons eu l'occasion d'analyser dans les pages précédentes.

À notre avis, aujourd'hui, nous pouvons identifier un ensemble d'outils d'encadrement de la circulation de l'information à caractère personnel, répondant à des natures très variées. Nous pouvons citer par exemple les guides destinées aux différents organismes publics et qui exposent clairement quelles sont les conditions de collecte, de transmission, de conservation et de destruction des renseignements personnels des citoyens. Pensons également aux ÉFVP, outil capable d'encadrer tout projet au sein des organismes du secteur public canadien, afin que les informations à caractère personnel fassent l'objet de la protection nécessaire.

Il est également essentiel d'évaluer le rôle de l'autoréglementation dans le champ de la protection des renseignements personnels, à cause de la nature même du droit à protéger. Certains soulignent à ce sujet :

> « […] nous pensons qu'il y a des contenus qui devraient échapper à l'autoréglementation, au nom de l'éthique et de la démocratie : l'interprétation de certaines valeurs ne peut être appropriée par des intérêts particuliers. Nous avons énoncé ailleurs le critère qui pourrait nous guider : dès que les intérêts de la majorité sont en jeu et dès que les citoyens risquent d'être fragilisés et rendus plus vulnérables, il y a lieu de

[859] P. TRUDEL, préc., note 222, p. 386.

> prévoir l'intervention publique pour maintenir ouvert "l'horizon d'universalité" qui caractérise l'éthique démocratique. »[860]

Mais en même temps, la thèse du pluralisme n'est plus capable par elle seule, d'encadrer les travaux relatifs au droit des nouvelles technologies de l'information, comme il l'a fait dans le passé. C'est à cause de la complexité du droit actuel que la thèse de l'existence du droit post-moderne peut rendre possible une analyse beaucoup plus complète des enjeux juridiques liés aux nouvelles technologies de l'information. Cela s'avère possible grâce à d'autres caractéristiques du droit post-moderne que nous analyserons par la suite.

Pluralité des phénomènes, pluralité d'acteurs dans le processus de création des normes, pluralité d'options. L'État fait partie aussi de cet ensemble et l'ordre juridique étatique va jouer un rôle essentiel dans la régulation de ces nouveaux phénomènes : « […] l'État conserve en effet une position centrale par rapport aux autres ordres juridiques, auxquels il est en mesure d'imposer sa tutelle ou médiation ; et la complexification des processus de production du droit n'est pas telle qu'elle sape une hiérarchie des normes qui apparaît consubstantielle au système de l'État du droit».[861] Nous considérons que cette affirmation s'accommode parfaitement bien du contexte des instruments de protection des renseignements personnels aujourd'hui, au moment où des lois, directives européennes, guides, lignes directrices et recommandations, entre autres, cohabitent, non sans une relation basée parfois sur le critère de la hiérarchie.

De plus, nous observons qu'au Canada pour le secteur public et en Europe où des nouveaux textes de loi protecteurs des renseignements personnels sont attendus dans les prochaines années, il devient urgent d'introduire dans les lois et directives des droits, des principes, des procédures et des méthodes d'évaluation existant aujourd'hui au sein d'instruments très divers, et cela pour leur accorder la toujours contraignante « force de loi ».

---

[860] Jacques BERLEUR et Tanguy EWBANK DE WESPIN, « Gouvernance de l'Internet : réglementation, autorégulation, corégulation ? », dans *Gouvernance de la société de l'information*, Cahiers du Centre de Recherches Informatique et Droit, num. 22, Bruxelles, Bruylant, 2002, p. 35 et 36 (nous soulignons).

[861] J. CHEVALLIER, préc., note 843, 675.

**B- Un droit négocié et en évolution constante**

Le droit post-moderne est un droit « négocié » parce que la force de la règle de droit dépend du consensus dont elle est entourée et, pour que cela soit possible, les destinataires de la règle vont devoir participer à son élaboration. Nous parlons d'un genre de légitimité procédurale, parce que les modes d'élaboration des règles deviennent essentielles à l'époque post-moderne où la délibération et le dialogue confèrent une légitimité nouvelle à la règle de droit.

Nous pouvons constater que ce besoin de consensus et de concertation trouve son origine dans la crise de la raison juridique :

> « Foncièrement marqué par l'unilatéralité, le droit apparaissait comme l'expression d'un "ordre hétéronome", auquel il était, non seulement impossible de se soustraire, mais encore nécessaire et juste de se soumettre. "Systématicité" et "normativité" étaient ainsi indissolublement liées. La crise de la Raison juridique a compromis cette efficacité normative : la force de la règle de droit ne provient plus de ce qu'elle s'énonce comme un ordre obligatoire, auquel tous sont tenus de se soumettre ; elle dépend désormais du consensus dont elle est entourée. Ce consensus suppose que les destinataires soient partie prenante à son élaboration : la concertation préalable, la participation à la définition de la règle devient la caution de son bien-fondé ; le droit devient ainsi un "droit négocié", qui est le fruit d'une délibération collective. À une légitimité intrinsèque, fondée sur la représentation du droit comme incarnation de la Raison, succède une "légitimité procédurale", attesté par ses modes d'élaboration. »[862]

Plusieurs acteurs sont appelés à participer au processus d'élaboration des normes (représentant des groupes de pression et des associations, experts sociaux, etc.) afin de négocier le contenu, l'étendue et la formulation des règles. Nous pouvons constater que le citoyen est appelé de plus en plus à prendre part à ce processus et que la participation des citoyens est presque devenue une étape nécessaire au processus législatif.

Bien que parfois la voix du citoyen ne soit pas toujours entendue et que les instruments normatifs adoptés aujourd'hui pour encadrer l'utilisation des technologies de l'information n'ont pas fait l'objet d'un débat ou d'une

[862] *Id.*

concertation publique, nous observons que de plus en plus de consultations ayant pour objectif d'identifier les demandes de la société ont lieu aujourd'hui.

La position renforcée qu'occupe le citoyen aujourd'hui trouve son origine dans la volonté de trouver dans la démocratie participative un modèle où le débat entre les citoyens et les pouvoirs publics devient une réalité. Ces derniers temps nous observons que les nouvelles technologies peuvent jouer un rôle important dans le processus de consultation, dès lors qu'elles offrent au citoyen la possibilité de participer via Internet aux différents débats qui ont lieu avant l'adoption des lois. Ces processus qui offrent la possibilité au citoyen de s'exprimer sur une matière ne sont pas exempts de certains risques qui doivent être pris en considération par les responsables des outils de consultation[863].

Le système de protection des renseignements, capable d'encadrer leur circulation dans le réseau, va devoir répondre, plus que jamais, à l'image d'un droit négocié. P. Trudel souligne cette idée du droit négocié qui naît du dialogue entre l'administration et le citoyen grâce à la mise en place de l'État en réseau, grâce auquel l'interaction État-citoyen peut s'accentuer :

> « La règle empêchant la circulation et la réutilisation des informations pour le motif que celles-ci pourraient être détournées de leur finalité, doit être relue dans le cotexte de dialogue accru que permet le réseau. Plus que jamais, l'Administration est en mesure d'indiquer à chaque administré quelles sont les informations qu'il possède sur son compte, lesquelles il entend utiliser afin de prendre une décision. Le citoyen est désormais en mesure d'interagir et d'exiger le retrait et l'ajout des informations. »[864]

Certains auteurs affirment que le droit contemporain répond à la logique informatique du « traitement de texte »[865]. Deux raisons peuvent être retenues à

---

[863] Pierre TRUDEL, Karim BENYEKHLEF, France ABRAN, Cynthia CHASSIGNEUX, Rosario DUASO CALÉS, Richard LANGELIER, *Guide pour maîtriser les risques juridiques des cyberconsultations*, Document préparé pour le Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles du Secrétariat du Conseil du Trésor et le Groupe de travail sur la Cyberdémocratie, Gouvernement du Québec, Novembre 2004.

[864] P.TRUDEL, préc., note 148, p. 18.

[865] François OST, « Le temps virtuel des lois post-modernes ou comment le droit se traite dans la société de l'information », dans Jean CLAM et Gilles MARTIN (dir.), *Les transformations de la régulation juridique*, Paris, L.G.D.J., 1988, 423, 427.

cela : le fait que le texte est en état de réécriture permanente et le fait qu'il renvoie à un nombre indéfini d'auteurs, « peut-être même à une absence d'auteur »[866]; F. Ost se demande même si le modèle de l'émetteur et du récepteur n'est pas plutôt subverti, parce que dans l'interactivité du réseau, les rôles s'échangent très facilement. Il s'interroge : « Y a-t-il un législateur dans le Parlement ? On sait que le développement de la technologie informatique permet aujourd'hui à la fois l'écriture en réseau (courrier électronique) et la participation interactive à la constitution de gigantesques banques de données (consultation d'Internet, par exemple, mais aussi contribution à son extension) ».[867]

Pour ce qui est de la « réécriture constante » de ce droit, nous constatons effectivement un besoin qui répond à ce besoin d'une « adaptation réseautique », nécessaire dans un contexte toujours changeant. En effet, un droit capable d'évoluer et de changer au fur et à mesure en assurant une protection « évolutive », à l'image des évolutions et des changements opérés dans le réseau devient nécessaire.

Ainsi, si la Directive du Conseil du Trésor de 2010 sur l'ÉFVP[868] établit que les organisations gouvernementales canadiennes auront la responsabilité « d'examiner annuellement l'annexe C (de cette Directive) afin de s'assurer que l'ÉFVP de base demeure pertinente et proposer des amendements si requis »[869]. Nous observons alors que cet instrument oblige à une évaluation annuelle de l'ÉFVP de base, qui répond à un modèle d'évaluation qui doit demeurer pertinent et actuel, grâce à des ajouts et des changements au besoin.

### C- Un droit produit en réseau

Nous pouvons vérifier que, de plus en plus, le droit est produit « en réseau », et cela grâce aux nouvelles techniques de communication et de négociation qui sont à l'origine de transformations dans élaboration du droit et qui nous font penser d'une certaine façon à une « construction collective ».

---

[866] *Id.*
[867] *Id.*, 429.
[868] SECRÉTARIAT DU CONSEIL DU TRÉSOR, préc., note 722.
[869] *Id.*, Point 8.1.4.

Mais cette élaboration en réseau répond également au besoin d'interaction de différents acteurs qui seront à l'origine de l'ensemble des mécanismes et des instruments de différentes natures devant contribuer à la « bonne gouvernance » des réseaux. En effet, « dans les espaces constitués par les réseaux, le cyberespace, la normativité s'élabore et s'applique selon un modèle réseautique »[870].

Le phénomène des « *norm entrepreneurs* » ou des « entrepreneurs normatifs », c'est-à-dire, « la contribution par la société civile à l'émergence et, éventuellement à la cristallisation des normes »[871], témoigne également de l'élaboration en réseau du droit actuel. En effet, ce concept fait plutôt référence au rôle majeur que des acteurs non étatiques ont aujourd'hui dans le processus de création des normativités. K. Benyekhlef fait référence à ce phénomène de « l'entrepreneur normatif » dans le contexte du droit du cyberespace :

> « Le champ du cyberespace se prête bien à l'élaboration par des acteurs non étatiques de normes propres à le réguler. Ce coup d'œil dans les *coulisses* de l'action normative est révélateur des temps actuels : un temps de mutation, de transformation des fondements du droit moderne sous le coup de phénomènes contemporains comme le cyberespace, le caractère global et anational des droits de la personne ou la mondialisation pour n'en citer que quelques uns. »[872]

Dans le contexte du droit relatif aux technologies de l'information ou droit du cyberespace, nous assistons effectivement à l'émergence de règles et d'autres mécanismes élaborés par des acteurs étatiques et non étatiques. De plus, le droit relatif à la protection des renseignements personnels dans les réseaux témoigne également de ces multiples acteurs dans le processus d'élaboration des normativités. Voici comment certains auteurs voient le phénomène de la création du droit en réseau :

---

[870] P. TRUDEL, préc., note 717 (nous soulignons).

[871] Karim BENYEKHLEF, « La résolution en ligne des différends de consommation : un récit autour (et un exemple) du droit postmoderne », dans Pierre-Claude LAFOND (dir.), *L'accès des consommateurs à la justice*, Yvon Blais, Cowansville, 2010, 89, p. 94.

[872] *Id.*

> « (...) un passage vers un droit multiple et hyper coopératif où la substance du droit revient dans la complexité du social. Elle serait reliée aux notions de complexité juridique. Or, diverses observations laissent supposer que la création du droit pourrait, du fait d'Internet, emprunter ce chemin du réseau. »[873]

En effet, il est question ici d'une certaine « complexité du social », accompagnée d'une certaine « complexité du droit » relatif au réseau qu'est Internet. Il est intéressant de voir que certains signalent qu'un « système complexe et constitué d'un grand nombre d'entités en interaction qui empêchent l'observateur de prévoir sa rétroaction, son comportement ou son évolution par le calcul »[874].

Définition qui nous semble très pertinente dans le contexte de la circulation des renseignements personnels dans les réseaux, puisque la notion de « réseau » s'accommode assez bien de cette image de « système complexe ».

En effet, la complexité du réseau aura un reflet dans le droit relatif aux réseaux et plus concrètement dans le droit d'Internet. Ce droit, qui a pour mission d'encadrer les activités se déroulant dans les réseaux, peut répondre à l'idée d'un droit, qui est un « système adaptatif complexe », qui va contribuer à une meilleure coordination des actions mais qui va se complexifier[875]. Ce droit « en réseau » nous semble *a priori* un droit plutôt complexe, pouvant certainement aider à apporter de la « prédictibilité » aux comportements se déroulant dans le réseau et servant surtout à encadrer les activités dans ce contexte.

Pour D. Bourcier, « la complexité loin d'être un handicap devient une ressource cognitive quand on trouve les représentations adéquates des interactions dynamiques que génère tout système qui évolue en s'adaptant »[876]. À notre avis, cette complexité du droit va effectivement pouvoir contribuer à la nécessaire « adaptation réseautique » et cela, grâce à un droit qui est formé par des

---

[873] Renaud BERTHOU, *L'évolution de la création du droit engendrée par Internet : vers un rôle de guide structurel pour l'ordre juridique européen*, thèse de doctorat, Rennes, Université de Rennes I, 2004 (nous soulignons).

[874] Danièle BOURCIER, *Sciences du droit, complexité, serendipité*, Exposé dans le cadre de l'Atelier Complexité et Politiques Publiques, 23-24 septembre 2010, en ligne : http://complexitejuridique.files.wordpress.com/2010/09/atelier-complexite-droitcomplexite-serendipite4.ppt#1 (consulté le 2 février 2011).

[875] *Id.*

[876] Danièle BOURCIER, *Sciences juridiques, complexité, serendipité*, Résumé de l'exposé dans le cadre de l'Atelier Complexité et Politiques Publiques, 23-24 septembre 2010.

mécanismes et des outils mises en place par des acteurs différents et qui ont pour vocation de s'adapter et d'évoluer constamment.

Comme nous pouvons le constater, cette conception du droit pluriel, négocié et constitué comme un réseau mais aussi créé en réseau, joue un rôle important dans nos recherches. En effet, dans le travail d'identification des mécanismes pouvant servir à la création d'un cadre de gouvernance adéquat pour protéger le droit à la vie privée dans les structures en réseau, cette conception du droit ouvre la voie à la recherche des outils les plus efficaces.

### D- Un droit souple, flou et mou

De plus, ce droit de la post-modernité est un droit « souple », en opposition au droit moderne, toujours conçu comme un ordre de contrainte. Il s'agit de plus en plus d'un droit dépourvu de la dimension contraignante spécifique du droit moderne. C'est aussi à cause de la façon de « négocier » le droit que nous pouvons constater que le consentement ou l'acceptation de la règle par les destinataires a des effets très positifs pour ce qui est du respect de ces règles.

Ces dernières années, nous assistons à la naissance d'un droit qui prend la forme de « lignes directrices » et de « recommandations ». Prenons l'exemple de l'OCDE, comme institution qui propose des objectifs à travers l'élaboration de lignes directrices portant sur des sujets divers. De la même façon, les directives européennes établissent des principes généraux que les États membres devront suivre à l'heure de légiférer. Dans le contexte du droit relatif à la protection des renseignements personnels, nous constatons également que certains « guides » constituent un outil de plus en plus utilisé à l'heure d'encadrer la circulation des renseignements personnels.

Comme J. Chevallier l'a dit, ce droit doux, est aussi un droit « flou » : des objectifs, des principes, des standards, qui finalement vont faire en sorte que le droit devienne quelque chose de moins précis. Cependant, nous ne concevons plus ces instruments autrement : même si le droit présente une certaine incertitude à cause de sa formulation, nous ne pouvons pas dire qu'il est moins efficace.

Nous avons pu démontrer que l'utilisation des standards dans le contexte du droit des technologies de l'information, et notamment dans le droit relatif à la protection des renseignements personnels, est un fait. En effet, ces standards et principes constituent un élément important du droit relatif à la protection des renseignements personnels et ne font que réaffirmer le besoin d'une adaptation constante à une réalité toujours changeante.

De plus, comme certains l'ont souligné, ce « flou du droit » va permettre de passer « d'un ordre à l'autre, en transcendant le pluralisme des foyers de droit, par la référence à des principes communs et transversaux »[877].

En effet, plus que jamais, nous pouvons compter sur un ensemble de principes généraux qui sont présents dans l'articulation des différents instruments normatifs. Si nous pensons aux principes généraux en matière de protection des renseignements personnels que la Directive 95/46/CE en la matière établit et aux lignes directrices de l'OCDE relatives à la protection de la vie privée, nous notons que les principes et orientations que ces deux dispositifs proposent ont tendance à devenir universels.

Nous pouvons dire que ces orientations, en matière de protection de la vie privée, sont à l'origine d'une culture de la protection des renseignements personnels. Nous observons que ces principes sont présents dans les textes de loi et les règlements en la matière, dans les politiques de confidentialité des différents sites Internet, dans les codes de conduite de plusieurs groupes professionnels, etc.

Ce droit de la post-modernité est aussi un droit « mou » et nous pouvons affirmer que cette caractéristique a des conséquences importantes sur le concept classique du droit et qu'elle implique surtout un grand degré d'incertitude quant aux frontières du droit. Aujourd'hui, le juridique et l'extra-juridique se mélangent plus que jamais. Les normes juridiques et les normes de natures différentes (technique, éthique, etc.) ne sont plus en opposition mais en combinaison, et nous pouvons voir que les unes vont influencer les autres.[878]

---

[877] J. CHEVALLIER, préc., note 10, p. 128.

[878] *Id.,* p.129.

J. Chevallier souligne l'idée suivante : « tandis que la juridicisation des standards techniques est indispensable pour leur donner leur plein effet, la technicisation de la norme juridique contribue à

Des moyens techniques destinés à éviter certains détournements de finalité dans le contexte du partage d'informations sur les citoyens entre les différents organismes peuvent être combinés à d'autres moyens normatifs afin de garantir l'effectivité du principe de finalité à l'égard de la protection des renseignements personnels. Il est intéressant de voir que la loi est parfois celle qui oblige à l'utilisation de certains moyens techniques afin d'assurer le respect de certains droits[879]. Les moyens normatifs et les moyens techniques s'accommodent et s'appuient les uns sur les autres dans le but de créer le cadre de protection le plus adapté aux environnements en réseau. Il faut noter que la question de la « neutralité technologique »[880] dans les lois présente sans aucun doute une des matières à réflexion les plus intéressantes aujourd'hui, posant des questionnements juridiques pouvant avoir un impact majeur dans le cadre de cette nouvelle gouvernance.

Le mélange du droit avec le non droit nous conduit à nous interroger sur la pertinence du droit étatique en tant que dispositif de régulation, comme conséquence de certaines évolutions techniques et scientifiques auxquelles nous assistons depuis quelques années. J. Chevallier précise à propos de l'encadrement relatif à Internet par le droit étatique classique :

> « Les difficultés de régulation d'Internet sont à cet égard exemplaires : elles témoigneraient, non seulement de l'incapacité de l'État à saisir un objet dématérialisé n'ayant pas de contact avec un

---

conforter; ainsi, la normativité juridique vient-elle se sur-imposer à la normativité technique, en redoublant ses effets ».

[879] *Loi concernant le cadre juridique des technologies de l'information,L.R.Q., chapitre C-1.1*. L'article 24 de cette loi oblige à prendre des mesures techniques en vue de préserver la finalité qui a motivé qu'un document soit rendu public : **«** L'utilisation de fonctions de recherche extensive dans un document technologique qui contient des renseignements personnels et qui, pour une finalité particulière, est rendu public doit être restreinte à cette finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés. Elle peut en outre, eu égard aux critères élaborés en vertu du paragraphe 2° de l'article 69, fixer des conditions pour l'utilisation de ces fonctions de recherche ».

[880] Voir sur la question de la neutralité technologique : Vincent GAUTRAIS, *Fictions et présomptions : outils juridiques d'intégration des technologies*, Présentation dans le cadre de la Conférence « Sécurité juridique et sécurité technique : indépendance ou métissage » organisée par le Programme international de coopération scientifique (CRDP / CECOJI), Montréal, 30 septembre 2003, en ligne : http://www.lex-electronica.org/docs/articles_105.pdf (consulté le 14 décembre 2010).

> territoire, mais aussi de l'inadéquation des catégories juridiques classiques. »[881]

**E- Un droit transitoire**

En même temps, certains auteurs ont déjà souligné le rythme de plus en plus accéléré du changement juridique, qui trouve son origine dans certains phénomènes nouveaux, comme celui de la diffusion sur Internet des informations qui, dans le passé, étaient publiées exclusivement en version papier, ou celui de la circulation de l'information entre les différents organismes publics afin d'offrir des prestations électroniques de services aux citoyens. Nous pouvons évoquer également le phénomène du *cloud computing* ou « informatique dans les nuages » que nous avons évoqué dans les pages précédentes et qui va sans doute changer le panorama actuel pour ce qui est des risques pour la protection effective des informations circulant dans le secteur public[882].

Nous pouvons dire qu'aujourd'hui « le transitoire est devenu l'habituel, l'urgence est devenue permanente »[883]. De plus en plus, le droit est « transitoire » et il est modifié quand cela s'avère nécessaire, ce qui devient très habituel à cause des changements rapides qui trouvent parfois leur origine dans les nouvelles technologies. Mais l'urgence est aussi la règle générale, et le droit, plus que jamais, est appelé à répondre aux besoins que la société et la réalité demandent. F. Ost souligne cette idée :

> « Or donc le droit s'est mis à courir. Si poser la question de savoir dans quelle direction il court, ou dans quel but, n'apparaît plus comme une interrogation juridique pertinente, c'est qu'effectivement un changement de paradigme s'est opéré. Le changement l'emporte sur la stabilité, l'instantané refoule la durée. »[884]

---

[881] J. CHEVALLIER, préc., note 10, p. 129.
[882] Voir à ce sujet : H. LE CROSNIER, préc., note 679.
[883] F. OST, préc., note 865, 424.
[884] *Id*, p. 425.

**F- Un droit réflexif**

Ce droit post-moderne est aussi un droit « réflexif », parce qu'après une évaluation et l'obtention de résultats, certains mécanismes de correction ont été mis en place pour essayer d'adapter le droit aux besoins réels et tenter de corriger ses imperfections. Nous l'avons vu, il existe une volonté d'évaluer les effets potentiels du droit, pendant son processus d'élaboration, mais aussi une volonté et un besoin d'évaluer le droit en vigueur.

Ainsi, la Loi Antiterroriste[885] sanctionnée en 2001 au Canada établit à son article 145 qu'un comité du Parlement doit effectuer dans les trois ans suivant sa sanction, un « examen approfondi des dispositions et de l'application » de la loi donnant comme résultat un rapport pouvant contenir des recommandations concernant des possibles modifications au texte de loi.

Il s'agit d'évaluer la pertinence de chaque texte de loi, d'analyser ses effets et les bénéfices des dispositions adoptées. F. Ost et M. Van de Kerchove parlent d'une dilution substantielle de la souveraineté de la loi qui est accompagnée d'une perte des qualités associées à sa prééminence. Ces auteurs nous rappellent que le *postulat de la rationalité du législateur* « cède aujourd'hui la place à l'idée d'une évaluation de plus en plus nécessaire et d'une censure toujours possible »[886].

Les mécanismes de réévaluation des lois et des outils de protection des renseignements personnels dans les réseaux nous semblent de plus en plus nécessaires : plus que jamais, le seul droit capable d'encadrer la protection des droits dans les nouveaux environnements doit pouvoir répondre en temps réel aux besoins. En effet, l'adaptation réseautique passe par ce type de mécanismes et par la capacité de réaction des instruments de gouvernance.

**G- Un « autre » droit**

Mais, ce droit post-moderne est aussi un droit qui comporte de nouvelles formes de réglementation. Dans la culture juridique post-moderne, nous reconnaissons

[885] L.C. 2001, ch. 41.
[886] F. OST et M. Van de KERCHOVE, préc.,note 845, p. 87.

plusieurs indices de complexité et des changements, que F. Ost analysait au moment de parler du modèle de juge Hermès : « On dérèglemente, mais ce n'est qu'une manière de reréglementer autrement, on dépénalise, mais c'est plus souvent au profit du redéploiement d'autres mesures coercitives, telles la médicalisation ou la fiscalisation des comportements indésirables, on déjudiciarise, mais c'est pour aussitôt mettre en place des mécanismes d'expertise, de conciliation, de médiation ou d'arbitrage »[887].

Pensons effectivement à la mise en place de mécanismes de règlement en ligne des conflits, qui ont bouleversé la négociation, la médiation et l'arbitrage classiques et qui semblent une voie naturelle dans le contexte de la nouvelle économie où les transactions se nouent de plus en plus dans les réseaux du cyberespace[888]. De plus, il faut souligner que pour K. Benyekhlef la résolution en ligne des différends de consommation constitue un exemple de droit post-moderne, comme il l'a affirmé dans un de ses articles sur la question[889].

Nous considérons que, dans le contexte de ce droit devant encadrer la protection des renseignements personnels, la théorie de la post-modernité peut représenter le cadre idéal pour appréhender les phénomènes juridiques à venir. La théorie du pluralisme juridique permettait déjà une analyse de ces phénomènes. Mais aujourd'hui, l'analyse des enjeux que le droit des nouvelles technologies de l'information présente et présentera ne peut pas se faire exclusivement selon la perspective de l'existence d'une pluralité d'ordres juridiques.
Nous en avons vu la raison : le droit post-moderne est un droit pluriel, pourtant il est aussi un droit négocié, souple, mou et réflexif. Nous assistons au passage d'un droit qui n'est plus structuré en pyramide, mais en réseau et qui est aussi formé en réseau. Nous parlons d'un droit où les changements s'opèrent fondamentalement

[887] François OST, « Jupiter, Hercule, Hermès : trois modèles du juge », dans Pierre BOURETZ (dir.), *La force du droit*, Paris, Éditions Esprit, 1991, p. 263.
[888] Voir à ce sujet : Karim BENYEKHLEF et Fabien GÉLINAS, *Le règlement en ligne des conflits. Enjeux de la cyberjustice*, Paris, Éditions Romillat, 2003, p. 66 et s.
[889] K. BENYEKHLEF, préc., note 471.

dans les nouvelles modalités de la régulation juridique, qui proviennent de certaines transformations qui se produisent aujourd'hui sur plusieurs niveaux.

Comme certains auteurs l'ont souligné, « le réseau est la forme dans laquelle peut se glisser un droit souple, flou, incertain et aléatoire »[890]. Cependant, nous ne pouvons pas nier l'existence de certains risques qui tirent leur origine des caractéristiques de ce droit :

> « Le risque existe évidemment que ce droit en réseaux, qui n'est plus soumis aux principes juridiques gouvernant la formation du droit autoritaire et hiérarchisé, se développe dans un vide juridique complet. Et c'est une tâche majeure de la doctrine de repenser le cadre du développement de ce droit. Il ne s'agit pas seulement, comme on l'a fait à ce jour, d'atténuer les exigences relatives à la formation du droit pour tenir compte de la souplesse et de la réflexivité inhérentes aux régulations. Il s'agit surtout d'élaborer des principes, des règles et des institutions mieux adaptées à leur mode opératoire et à leur structuration en réseaux. »[891]

Nous considérons que les questions relatives à la protection des renseignements personnels dans les structures réseautiques peuvent être étudiés assez convenablement à l'aide des théories dont nous avons fait référence dans les lignes précédentes. Plus que jamais, il est important d'analyser les fondements et le sens du principe de finalité sous un angle relatif à un droit qui ne revêt plus les caractéristiques du droit classique.

Nous pouvons affirmer que la post-modernité du droit a changé la donne et que ce cadre présente des caractéristiques qui s'adaptent très bien aux besoins du contexte réseautique qui est au centre de nos travaux. Nous avons pu constater que le droit relatif à la protection des renseignements personnels est voué à être toujours efficace dans des contextes toujours changeants, ce qui va nous faire passer de notions fixes vers d'autres notions plus contemporaines, beaucoup plus dynamiques et souples.

L'existence de standards dans le droit sur la protection de la vie privée dans les réseaux est révélatrice de la manière dont ce droit opère. De plus, l'existence de

---

[890] C.-A. MORAND, préc., note 19, p.208.

[891] *Id*, p. 207 (nous soulignons).

nouveaux standards peut être à l'origine d'un cadre de protection capable d'aider à la protection des informations dans le contexte des réseaux. Ces standards et nouveaux standards doivent sans doute servir à garantir une « adaptation réseautique » du droit relatif à la protection des renseignements personnels, qui aidera sans doute à neutraliser les risques dérivés des nouveaux et nombreux flux d'informations dans le secteur public.

## CONCLUSION

Nous constatons qu'est aujourd'hui nécessaire une application effective du principe de finalité afin de créer des règles adéquates au modèle d'État en réseau, caractérisé notamment par « le partage et l'échange d'informations civiles, ce qui devraient permettre de simplifier les démarches des citoyens »[892].
Il est clair que la transformation de l'administration présente, d'une part, l'enjeu du « décloisonnement vertical au sein d'une même administration, décloisonnement réducteur de certaines pesanteurs hiérarchiques »[893] et que, d'autre part, il existe surtout un « décloisonnement horizontal, entre administrations »[894] qui va avoir des conséquences majeures sur la conception classique de l'administration et qui témoigne d'une véritable mutation dans l'organisation des structures administratives les plus traditionnelles.

Les objectifs d'efficacité de l'action administrative grâce à l'utilisation des nouvelles technologies de l'information et de la communication[895], l'amélioration de la relation administration-administrés par l'informatique[896] et le « développement d'une offre de qualité de services en ligne de l'administration exige une mise en réseau renforcée des services de l'État »[897].

Si dès 1980 certaines voix ont affirmé que « l'informatique a fait de la vie privée un des problèmes capitaux de notre temps »[898], nous pouvons comprendre qu'Internet

---

[892] Katia DUHAMEL, *Les collectivités territoriales et les communications électroniques, Initiatives, droit et contrats*, Paris, Éd. Du Moniteur, 2006, p. 278.
[893] Jean -Noël TRONC, « L'administration et les technologies de l'information et de la communication » dans Danielle BAHU-LEYSER et Pascal FAURE (dir.), *Nouvelles technologies, Nouvel État*, Paris, La Documentation Française, 1999, 151, p. 157.
[894] *Id.*
[895] SECRÉTARIAT D'ÉTAT AUPRÈS DU PREMIER MINISTRE CHARGÉ DE LA FONCTION PUBLIQUE ET DES SIMPLIFICATIONS ADMINISTRATIVES, *La mutation de l'administration, objectifs et conditions*, Paris, La Documentation Française, 1986, p. 48.
[896] Lire à ce sujet : Françoise GALLOUEDEC-GENUYS, *Une informatique pour les administrés ?*, Paris, Éd. Cujas, 1980, p. 107.
[897] J.–N. TRONC, préc., note 893, p. 157.
[898] Françoise GALLOUEDEC-GENUYS, « La vie privée : une création informatique », dans Françoise GALLOUEDEC-GENUYS et Philippe LEMOYNE (dir.), *Les enjeux culturels de l'informatisation*, Paris, La Documentation Française, 1980, 65, p. 74.

et la mise en place de structures réseautiques comme celle de l'État ne font qu'amplifier le phénomène.

Si le principe de finalité a pour un de ses effets les plus directs l'interdiction faite aux organismes de communiquer ou céder les renseignements personnels à des tiers non autorisés[899], il est important de souligner que la « contrepartie de l'obligation des administrés de communiquer à l'administration des informations, parfois très intimes, est l'obligation qu'a l'administration de ne pas utiliser des informations à des fins autres que celles prévues à l'origine »[900].

Nous avons analysé que l'avènement des structures en réseau venant remplacer des architectures en silo existant par le passé n'ont fait que changer le scénario des modalités de circulation des renseignements personnels.

De plus, certains phénomènes tels que l'utilisation de l'informatique dans les nuages ou l'implantation des applications Web 2.0 dans les sites du gouvernement, présentent des enjeux majeurs pour ce qui est de la protection des renseignements personnels dans le contexte de l'État en réseau et de « l'administration publique virtualisée »[901].

Si nous pouvons affirmer la pertinence des principes classiques de protection des renseignements personnels dans ce contexte, nous sommes en mesure d'affirmer la grande importance du principe de finalité, notamment comme instrument de gouvernance des réseaux.

Si la notion de finalité a été adoptée par le législateur dans les différents instruments de protection des renseignements personnels visant à encadrer des problématiques liées à la protection de la vie privée avant même l'arrivée du grand réseau qu'est Internet, il est licite de se questionner sur ses capacités à encadrer de nouveaux phénomènes.

---

[899] Voir : Bénédicte DELAUNAY, *L'amélioration des rapports entre l'administration et les administrés*, Paris, L.G.D.J., 1993, p. 319.
Bruno LASSERRE, Noëlle LENOIR et Bernard STIRN, *La transparence administrative*, Paris, PUF, 1987, p. 94.

[900] B. LASSERRE, N. LENOIR et B. STIRN, préc., note 899, p. 94.

[901] P. TRUDEL, préc., note 222, p. 376.

Cette réflexion qui a guidé nos recherches conduit clairement vers un constat qui nous semble apporter des réponses à nos questions initiales. En effet, par l'étude de la capacité des instruments, tels que les standards et les notions à contenu variable, nous pouvons comprendre que la notion de finalité renferme des qualités contribuant essentiellement au façonnement toujours nécessaire afin d'encadrer convenablement les structures réseautiques.

En effet, ce principe de finalité renferme des propriétés qui sont celles permettant une adaptation à des situations en mutation permanente et une capacité d'ajustement aux situations toujours évolutives qui engendrent des enjeux majeurs dans la gouvernance des réseaux.

Ce principe de finalité représente un élément qui s'accorde à la perfection aux théories relatives au droit post-moderne que nous avons étudié dans le cadre de nos travaux et que certains qualifient de « droit complexe en réseau »[902].

Pour F. Ost, ce droit post-moderne est un « ordre en réseau qui se traduit par une infinité d'informations à la fois instantanément disponibles et difficilement maîtrisables, comme peut l'être une banque de données »[903]. Cette image nous aide à comprendre comment ce droit en réseau se présente et quels sont ses attributs.

Les traits caractéristiques de ce principe de finalité s'accordent également bien à ce droit post-moderne qui est pluriel, négocié, en évolution constante, produit en réseau, souple, flou, mou, transitoire et réflexif.

De plus, c'est un droit flexible et cette « flexibilité du droit, se pliant à un rythme d'évolution propre à l'objet, est certes gage d'adéquation et d'acceptation des différentes évolutions »[904]. Ce droit qui suit et accompagne le rythme donné par le « réseau » est un droit en réseau formé par des normes en interaction et fait

---

[902] François OST, « Le rôle du droit : de la vérité révélée à la réalité négociée », dans Gerard TIMSIT, Alain CLAISSE et Nicole BELLOUBET-FRIER (dir.), *Les administrations qui changent, Innovations techniques ou nouvelles logiques ?*, Paris, PUF, 1996, 73, p. 78.

[903] *Id.*

[904] Marie-Anne FRISON-ROCHE, « Les rythmes dans l'évolution conjointe et commune des services publics », dans Jean-Marie CHEVALIER, Ivar EKELAND et Marie-Anne FRISON-ROCHE (dir.), *L'idée de service public est-elle encore soutenable ?*, Paris, PUF, 1999, 31, p. 36.

référence à une « nouvelle façon de concevoir un encadrement juridique, sans cesse mouvant, toujours provisoire, en attente perpétuelle de sa réforme »[905].
Nous observons ce phénomène à cause de l'impossibilité qui existe parfois de prévoir le caractère incertain des lois et nous constatons l'existence de lois expérimentales qui sont évaluées continuellement par des mécanismes que le législateur met en place à l'heure de légiférer.

Mais ce droit est également un droit « liquide »[906] qui va se présenter « en certaines occasions à l'état fluide, qui lui permet de se couler dans les situations les plus diverses et d'occuper ainsi en douce tout l'espace disponible, tout en s'accommodant, le cas échéant, de très fortes compressions »[907].

Ce droit nous fait penser également au concept de « souveraineté virtuelle »[908] que certains auteurs avancent et qui reposerait sur le paradigme du réseau, « dont le modèle analogique serait celui du réseau et qui aurait recours au réseau pour assurer leur action »[909].
Le cadre « réseautique », qui peut protéger les renseignements personnels dans les réseaux et offrir les instruments nécessaires à une gouvernance des risques informationnels, possède toutes les qualités caractérisant la conception du droit post-moderne. Les principes se trouvant à la base des systèmes de protection des renseignements personnels et représentant la pierre angulaire des législations en la matière deviennent les éléments clés de ces systèmes.

Toutefois, ces systèmes doivent pouvoir compter sur de nouveaux mécanismes d'adaptation réseautique capables d'opérer dans les environnements en réseau. Les

---

[905] *Id.*
[906] F. OST, préc., note 902, p. 81.
[907] *Id.*
[908] Karim BENYEKHLEF, « Vers une réformation de l'État-nation : vers une souveraineté virtuelle ? », dans Karim BENYEKHLEF et Pierre TRUDEL (dir.), *État de droit et virtualité*, Montréal, Éditions Thémis, 2009, 82, p. 83.
L'auteur parle d'une souveraineté « qui emprunterait alors les formes du réseau, analogie opératoire dans un univers pluraliste et polycentrique, et dont le déploiement serait facilité par les technologies de l'information et de la communication (Internet : le réseau des réseaux) ».
[909] *Id.*

pistes que nous avons analysées dans nos recherches afin d'identifier ces possibles mécanismes nous laissent penser que les ÉFVP, le *Privacy by Design*, les aires de partage ou le *Computer Grundrecht* entre autres, peuvent conformer le cadre actualisé capable de protéger les renseignements personnels effectivement. L'établissement et le renforcement de certains principes de protection peuvent venir compléter les instruments conformant une gouvernance adaptée aux besoins découlant du réseau.

En effet, ces « principes directeurs » sont dès lors un élément essentiel du droit en réseau et peuvent jouer un rôle permettant l'interaction entre les différentes normes :

> « Ainsi, le recours aux principes directeurs afin d'exprimer le droit reflète bien la structure en réseau du droit. À l'instar des réseaux de neurones, ils fournissent des liens permettant la mise en rapport de normes très diverses. Plutôt que de chercher et s'épuiser à uniformiser via des règles fixes, on va plutôt chercher à assurer la compatibilité des réglementations sur la base de divers principes à appliquer. »[910]

Ainsi, les nouveaux standards reliés au concept de finalité et aux différentes notions opérant dans la protection des renseignements personnels ne peuvent que contribuer à ce que le nouveau cadre de protection puisse s'adapter convenablement aux exigences d'un contexte toujours évolutif et en perpétuel changement.

Dans le contexte de l'État en réseau, nous ne pouvons pas oublier que « la protection de la vie privée n'est pas l'ennemi, mais l'ami dans l'exercice efficace de la prestation de services à tous les niveaux du gouvernement »[911]. Cette idée peut guider la réflexion devant conduire à d'éventuelles réformes des lois de protection des renseignements personnels voulant répondre aux besoins du gouvernement électronique. Comme certains auteurs l'ont souligné, « le mouvement actuel et

[910] P. TRUDEL, préc., note 222, p. 388.
[911] D. H. FLAHERTY, préc., note 262, p. 20.

prévisible de l'évolution du e-gouvernement requiert de penser autrement l'intervention du droit et les conditions de la gouvernance »[912].

Un nouveau modèle de gouvernance et le droit relatif à la protection des renseignements personnels pouvant encadrer convenablement les structures en réseau vont pouvoir se nourrir de certains mécanismes d'adaptation réseautique afin de répondre aux exigences présentes et futures.

[912] P. TRUDEL, préc., note 222, p. 379.

# BIBLIOGRAPHIE

## LÉGISLATION ET RÉGLEMENTATION

### *Textes constitutionnels*

Charte canadienne des droits et libertés, partie I de la *Loi constitutionnelle de 1982*, [annexe B de la *Loi de 1982 sur le Canada*, c. 11 (R.-U.)].

### *Textes fédéraux canadiens*

*Loi antiterroriste*, L.C. 2001, c. 41.

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

*Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.

### *Textes québécois*

*Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1.

*Loi sur l'administration publique*, L.R.Q., c.A-6.01.

### *Législation étrangère*

#### Belgique

*Loi relative à la protection de la vie privée l'égard des traitements de données à caractère personnel du 8 décembre 1992, (M.B. 8 mars 1998).*

#### Espagne

*Constitución Española de 1978*, BOE-A-1978-31229.

*Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal*, BOE-A-1999-23750.

*Ley Orgánica 58/2003, de 17 de diciembre, General Tributaria*, BOE-A-2003-23186.

#### États-Unis

*E-Government Act*, *Public Law* 107-347, 44 U.S.C. ch. 36.

**France**

*Loi relative à l'informatique, aux fichiers et aux libertés* (nº 78-17 du 6 janvier 1978), J.O. 7 janvier 1978 et rectificatif du 25 janvier 1978.

*Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (n° 2004-801du 6 août 2004) et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, J.O. nº 182 du 7 août 2004

**Union européenne**

*Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel du 28 janvier 1981 du Conseil de l'Europe,* S.T.E. nº 108.

*Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, JOCE 281 du 23 octobre 1995.

**Autres instruments**

OCDE, *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, adoptées le 23 septembre 1980.

Code type sur la protection des renseignements, CAN/CSA-Q380-F96 (C2001).

**JURISPRUDENCE**

***Jurisprudence canadienne***

*Cheskes c. Ontario* (Procureur général), (2007). O.J. Nº 3515.

*Eastmond c. Canadian Pacific Railway*, (2004) C.F. 852.

*Englander c. Telus Communications*, (2004) C.A.F. 387.

*La Reine c. Dyment,* [1988] 2 R.C.S. 417.

*Loi sur la protection des renseignements personnels (Can.) (Re),* [2000] 3 C.F. 82.

*Loi sur la protection des renseignements personnels (Can.) (Re),* [2001] 3 R.C.S. 905.

*R. c. Oakes* [1986] 1 R.C.S. 103.

*R. C. O'Connor*, [1995], 4 R.C.S.

***Jurisprudence étrangère***

*Sentencia 29/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

*Cour constitutionnelle fédérale allemande, Arrêt du 27 fèvrier 2008.*

**DÉLIBÉRATIONS DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS**

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n. 81-03 du 10 mars 1981 portant avis relatif à la création de traitements automatisés d'informations nominatives effectués sur la base des informations collectées à l'occasion du recensement général de la population de 1982.*

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n. 81-07 du 3 février 1981 portant avis relatif à la création d'un traitement automatisé d'informations nominatives concernant les titres de séjour des étrangers.*

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n. 81-74 du 16 juin 1981 portant décision et avis relatifs à un traitement automatisé des certificats de santé dans les services de la protection maternelle et infantile.*

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n. 81-88 du 21 juillet 1981 portant avis sur la mise en œuvre d'un traitement automatisé du répertoire national des entreprises et établissements (SIRENE).*

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n. 81-118 du 01 décembre 1981, portant avis relatif à l'utilisation du fichier de la taxe d'habitation par l'I.N.S.E.E. pour le recensement de la population en 1982.*

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n. 84-40 du 20 novembre 1984 relative au détournement du fichier de gestion du personnel sur ordinateur d'EDF-GDF.*

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n. 85-60 du 5 novembre 1985 portant recommandation relative à l'utilisation par les candidats aux élections politiques et les partis politiques de*

*fichiers publics et privés, en vue de l'envoi de documents de propagande et de la recherche de financement*.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n. 97-021 du 25 mars 1997 portant avis sur un projet d'article L. 115-8 du code de la sécurité sociale.*

## DOCTRINE

### *Monographies*

AGAMBEN, G., *État d'exception, Homo Sacer,* Paris, Éditions du Seuil, 2003.

ALLADAYE, R., *Petite philosophie du secret,* Toulouse, Éditions Milan, 2006.

BENYEKHLEF, K., *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Éditions Thémis, Montréal, 1992.

BENYEKHLEF, K., *Une possible histoire sur la norme*, Montréal, Éditions Thémis, 2008.

BENYEKHLEF K. et F. GÉLINAS, *Le règlement en ligne des conflits. Enjeux de la cyberjustice*, Paris, Éditions Romillat, 2003.

BENSOUSSAN, A., *Informatique, Télécoms, Internet*, Levallois, Éditions Francis Lefebvre, 2004.

BECK, U., *La société du risque, Sur la voie d'une autre modernité*, Paris, Aubier, 2001.

BOURCIER, D., *La décision artificielle : le droit, la machine et l'humain*, Paris, PUF, 1995.

BRAIBANT, G., *Données personnelles et société de l'information, Rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46*, Paris, La Documentation Française, 1998.

BRUGUIÈRE, J.-M., *Les données publiques et le droit*, Paris, Litec, 2002.

CASTELLS, M., *La société en réseaux, L'ère de l'information*, Paris, Fayard, 2001.

CARCENAC, T., *Pour une administration électronique citoyenne - méthodes et moyens*, Paris, La Documentation française, 2000.

CASTETS-RENARD, C., *Notions à contenu variable en droit d'auteur*, Paris, l'Harmattan, 2003.

CHASSIGNEUX, C., *Vie privée et commerce électronique*, Thémis, Montréal, 2004.

CHEVALLIER, J., *L'État post-moderne*, Paris, LGDJ, 2004.

CLUZEL-MÉTAYER, L., *Le service public et l'exigence de qualité*, Paris, Dalloz, 2006.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Dix ans d'informatique et libertés*, Paris, Economica, 1988.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Les libertés, et l'informatique, Vingt ans de délibérations commentées*, Paris, La Documentation française, 1996.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DE LIBERTÉS, *Voix, Image et Protection des Données Personnelles*, Paris, La Documentation Française, 1996.

DELAUNAY, B., *L'amélioration des rapports entre l'administration et les administrés*, Paris, L.G.D.J., 1993.

DE LAMBERTERIE, I. et H.-J. LUCAS (dir.), *Informatique, libertés et recherche médicale*, Paris, CNRS Éditions, 2001.

DUHAMEL, K., *Les collectivités territoriales et les communications électroniques, Initiatives, droit et contrats*, Paris, Éd. Du Moniteur, 2006.

FÉRAL-SCHUHL, C., *Cyber droit, Le droit à l'épreuve de l'Internet*, Paris, Dalloz, 2006.

FERNANDEZ SALMERON, M., *La protección de los datos personales en las administraciones públicas*, Madrid, Civitas, 2004.

FRAYSSINET, J., *Informatique, fichiers et libertés*, Paris, Litec, 1992.

GALLOUEDEC GENUYS F. et H. MAISL, *Le secret des fichiers*, Paris, Éditions CUJAS, 1976.

GALLOUEDEC-GENUYS, F., *Une informatique pour les administrés ?*, Paris, Éd. Cujas, 1980.

GAUTRAIS, V. et P. TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010.

GÉRIN, G., *Les effets de l'informatique sur le droit à la vie privée*, CEDAM, 1990.

KAYSER, P., *La protection de la vie privée par le droit*, Paris, Ed. Economica, 1995.

LAFFAIRE, M.-L., *Protection des données à caractère personnel*, Éditions d'organisation, Paris 2005.

LASSERRE B., N. LENOIR et B. STIRN, *La transparence administrative*, Paris, PUF, 1987.

MAISL, H., *Le droit des données publiques*, Paris, LDGJ, 1996.

MALLET-POUJOL, N., *Commercialisation des banques de données*, Paris, CNRS Éditions, 1993.

MALLET-POUJOL, N., (dir.), *Traçage électronique et libertés*, Problèmes politiques et sociales nº 925, Paris, La Documentation Française, 2006.

MANDELKERN, D. et B. DU MARAIS, *Diffusion des données publiques et révolution numérique*, Paris, La Documentation française, 1999.

MARLIAC-NÉGRIER, C., *La protection des données nominatives informatiques en matière de recherche médicale*, Tome II, Presses Universitaires d'Aix-Marseille, 2001.

MESSÍA DE LA CERDA BALLESTEROS, J. A., *La cesión o comunicación de datos de carácter personal*, Madrid, Civitas Ediciones, 2004.

MORAN, M., *Rethinking the Reasonable Person: An Egalitarian Reconstruction of the Objective Standard*, New York, Oxford University Press, 2003.

MORAND, C.-A., *Le droit néo-moderne des politiques publiques*, Paris, LGDJ, 1999.

NEWMAN, A. L., *Protectors of Privacy, Regulating Personal Data in the Global Economy*, Ithaca, Cornell University Press, 2008.

NIBLETT, G.B.F., *L'information numérique et la protection des libertés individuelles*, Paris, OCDE, 1971.

OPPETIT, B., *Droit et modernité*, Paris, PUF, 1998.

OST, F. et M. Van de KERCHOVE, *De la pyramide au réseau ?*, Bruxelles, Publications des Facultés universitaires Saint-Louis, 2002.

RIALS, S., *Le juge administratif français et la technique du standard (essai sur le traitement juridictionnel de l'idée de normalité)*, Paris, L.G.D.J., 1980.

ROULAND, N., « Anthropologie juridique », dans *Droit politique et théorique*, Paris, PUF, 1988.

ROUX, A., La protection de la vie privée dans les rapports entre l'État et les particuliers, Paris, Economica, 1983.

SANHOURY, A.A., *Les restrictions contractuelles à la liberté individuelle de travail dans la jurisprudence anglaise*, Paris, Marcel Giard, 1925.

SOLOVE, D. J., *Understanding Privacy*, Cambridge, Massachusetts, Harvard University Press, 2008.

STATI, M.O., *Le Standard juridique*, Paris, Librairie de jurisprudence ancienne et moderne, 1927.

TRUDEL, P., F. ABRAN, K. BENYEKHLEF et S. HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997.

TRUCHE, P., J.-P. FAUGÈRE et P. FLICHY, *Administration électronique et protection des données personnelles - Livre blanc*, Paris, La Documentation française, 2002.

VAN DROOGHENBROECK, S., *La proportionnalité dans le droit de la Convention européenne des droits de l'homme, Prendre l'idée simple au sérieux*, Bruxelles, Bruylant, Publ. FUSL, 2001.

VERBIEST, T. et E.WÉRY, *Le droit de l'Internet et de la société de l'information, Droits européen, belge et français*, De Boeck et Lancier, Bruxelles, 2001.

VITALIS, A., *Informatique, Pouvoir et Libertés*, Paris, Economica, 1981.

WALTER, J.-P., *La protection de la personnalité lors du traitement de données à des fins statistiques*, Fribourg, Éditions universitaires Fribourg-Suisse, 1988.

***Articles de revue et études d'ouvrages collectifs***

ASTIER, S., « Une régulation éthique de l'internet : les défis d'une gouvernance mondiale », (2005), *Revue Internationale des Sciences Administratives, L'e-gouvernance : défis et opportunités pour la démocratie, l'administration et le droit*, vol. 71-1, 143.

BENYEKHLEF, K., « L'administration publique en ligne au Canada : précisions terminologiques et état de la réflexion », (2004) *Revue française d'administration publique* n° 110, 267.

BENYEKHLEF, K., « La résolution en ligne des différends de consommation : un récit autour (et un exemple) du droit postmoderne », dans Pierre-Claude LAFOND (dir.), *L'accès des consommateurs à la justice*, Yvon Blais, Cowansville, 2010, 89.

BENYEKHLEF, K., « Vers une réformation de l'État-nation : vers une souveraineté virtuelle ? », dans Karim BENYEKHLEF et Pierre TRUDEL (dir.), *État de droit et virtualité*, Montréal, Éditions Thémis, 2009, 82.

BERLEUR J. et T. EWBANK DE WESPIN, « Gouvernance de l'Internet : réglementation, autorégulation, corégulation ? », dans *Gouvernance de la société de l'information*, Cahiers du Centre de Recherches Informatique et Droit, n° 22, Bruxelles, Bruylant, 2002, 35.

BOUDREAU, C., « À l'aube d'une transformation profonde de l'État », *Revue Télescope, Observatoire de l'administration publique de l'ENAP*, vol. 10, n° 5, novembre 2003, 2.

BOURCIER, D., « De l'intelligence artificielle à la personne virtuelle : émergence d'une entité juridique ? », *Droit et société*, 2001/3, n° 49, 847.

CADOUX, L., « La vidéosurveillance des lieux publics », dans *Nouvelles technologies de l'information et libertés individuelles*, Nathalie MALLET-POUJOL (dir.), Paris, La Documentation française, 1998.

CAPORAL, S., « Édouard Lambert, Théoricien de la Jurisprudence Sociologique », *Acta Universitatis Danubius Juridica*, n° 1/2009, 20, en ligne : "http://www.juridica-danubius.ro/continut/arhiva/A117.pdf" (consulté le 20 juin 2010).

CARBONNIER, J., « Les notions à contenu variable dans le droit français de la famille », dans Ch. PERELMAN et R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 1984, 99.

CATALA, P., « Unité ou complexité », dans *Droit et informatique, L'hermine et la puce*, Coll. Fredrik R. Bull, vol. 11, Paris, Masson, 1992.

CAVOUKIAN, A., *Privacy by Design* : *The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices*, 20 août 2009, en ligne : "http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf " (consulté le 11 avril 2011).

COLLECTIF D'AUTEURS (LIGUE DES DROITS DE L'HOMME, SYNDICAT DES AVOCATS DE FRANCE, *et al.*), *INES, de la suspicion au traçage généralisé*, dans *Traçage électronique et libertés*, Nathalie MALLET-POUJOL (dir.), *Problèmes politiques et sociaux nº 925*, Paris, La Documentation Française, 2006, 31.

CHEVALLIER, J., « L'ordre juridique », dans *Le Droit en procès*, Paris, PUF, 1983, 43.

CHEVALLIER, J., « Vers un droit post-moderne ?», *R.D.P.*, nº 3-1998, 660.

DACQUIR, B., « Le droit de la vie privée : aperçu général et règle de la proportionnalité », dans Benjamin DACQUIR et Andrée PUTTEMANS (dir.), *Actualités du droit de la vie privée*, Bruxelles, Bruylant, 2008, 27.

DEMERS, D.L., « Les concepts flous, l'interprétation constructiviste et la modélisation», dans Claude THOMASSET et Danièle BOURCIER (dir.), *Interpréter le droit : le sens, l'interprète, la machine*, Bruxelles, Bruylant, 1997, 221.

DEGRAVE, E., « Principe de finalité et secteur public dans la jurisprudence de la Commission de la protection de la vie privée », *Chroniques de droit public*, issue 1, 2009, 46.

DESGENS-PASANAU, G., « Informatique et Libertés : une équation à plusieurs inconnues », dans Jean-Luc GIROT (dir.), *Le harcèlement numérique*, Paris, Dalloz, 2005, 75.

DUASO CALÉS, R., « El derecho a la protección de los datos personales en el ámbito privado en la legislación federal canadiense y quebequense », dans Esther MITJANS et José Maria CASTELLA (dir.), *Derechos y Libertades en Canadá*, Barcelona, Ed. Atelier, Col. Canadiana, 2005, 355.

DUASO CALÉS, R., « Regulación europea sobre difusión de la jurisprudencia en Internet », dans Carlos GREGORIO et Sonia NAVARRO SOLANO (dir.), *Internet y sistema judicial en América Latina, Reglas de Heredia*, Buenos Aires, Ad-Hoc, 2004, 251.

DUASO CALÉS, R., « Redes sociales y vida privada: una ecuación posible », dans Carlos G. GREGORIO et Lina ORNELAS (dir.), *Protección de datos en las redes sociales digitales: en particular de niños y adolescentes*, México D.F., IFAI et IIjusticia, 2011, 195.

DUGUET, A.-M., « La collecte de données médicales et les échanges de données pour les recherches biomédicales et en santé publique. La législation française et ses conséquences sur l'évaluation des projets multicentriques » dans Jean HERVEG (dir.), *La protection des données médicales : les défis du XXè siècle*, Louvain-la-Neuve, Anthémis, 61.

FLICHY, P. et DAGIRAL, E., « L'administration électronique : une difficile mise en cohérence des acteurs », (2004) *Revue française d'administration publique* n° 110, 245.

FRISON-ROCHE, M.-A., « Les rythmes dans l'évolution conjointe et commune des services publics », dans Jean-Marie CHEVALIER, Ivar EKELAND et Marie-Anne FRISON-ROCHE (dir.), *L'idée de service public est-elle encore soutenable ?*, Paris, PUF, 1999, 31.

GALLOUEDEC-GENUYS, F., « La vie privée : une création informatique », dans Françoise GALLOUEDEC-GENUYS et Philippe LEMOYNE (dir.), *Les enjeux culturels de l'informatisation*, Paris, La Documentation Française, 1980, 65.

GAUTRAIS, V., « Le défi de la protection de la vie privée face aux besoins de circulation de l'information personnelle », *Revue Lex Electronica*, vol. 9, num. 2, Numéro Spécial, Été 2004, p. 2, en ligne : "http://www.lex-electronica.org/" (consulté le 17 février 2011).

GENTOT, M., « Administration électronique et protection de la vie privée : Renouveau de la problématique», dans George CHATILLON et Bertrand DU MARAIS (dir.), *L'administration électronique au service des citoyens*, Bruxelles, Bruylant, 2003, 325.

GEORGES, M., « Protéger les données à l'heure des réseaux », dans *Liberté, Risque et Responsabilité*. Nouveaux repères à l'heure de la mondialisation et du terrorisme international, CAHIERS DE L'IFRI, Paris, La Documentation française, 2002, 1116.

GHESTIN, J., « L'ordre public, notion à contenu variable, en droit privé français», dans Ch. PERELMAN et R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 1984, 77.

KEATS CITRON, D., « Fulfilling Government 2.0's Promise with Robust Privacy Protections », 78 *George Washington Law Review*, A-101 (2010).

KERNAGHAN, K., « L'évolution vers l'état virtuel : intégration des services et des canaux de prestations des services en vue d'une prestation axée sur le citoyen », (2005), *Revue Internationale des Sciences Administratives, L'e-gouvernance : défis et opportunités pour la démocratie, l'administration et le droit*, vol. 71-1, 129.

KERWER, D., "Rules that Many Use : Standards and Global Regulation", *Governance : An International Journal of Policy, Administration and Institutions*, vol. 18, n° 4, 2005, en ligne : "http://onlinelibrary.wiley.com/doi/10.1111/j.1468-0491.2005.00294.x/abstract" (consulté le 6 juillet 2010).

LAU, E., « Principaux enjeux de l'administration électronique dans les pays membres de l'OCDE », (2004) 110 *Revue française d'administration publique*, 225.

LECLERQ, P., « La Cnil, garante de la finalité, de la loyauté et de la sécurité des données personnelles », dans Marie-Christine PIATTI (dir.), *Les libertés individuelles à l'épreuve des NTIC*, Lyon, Presses Universitaires de Lyon, 2001, 111.

LEGROS, R., « Les notions à contenu variable en droit pénal », dans Ch. PERELMAN et R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 1984, 21.

LEPAGE, A., « Consentement et protection des données à caractère personnel », dans Jean-Luc GIROT (dir.), *Le harcèlement numérique*, Paris, Dalloz, 2005, 227, p. 248.

LEVIN, A., M. J. NICHOLSON, « Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground», 2:2 UOLTJ, 357 (2005), 391.

MAISL, H. « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager », dans George CHATILLON et Bertrand DU MARAIS (dir.), *L'administration électronique au service des citoyens*, Bruxelles, Bruylant, 2003, 349.

MAISL, H., « État de la législation française et tendances de la jurisprudence relatives à la protection des données personnelles », *Revue internationale de droit comparé*, Vol. 39 n. 3, 1987, 559.

MALLET-POUJOL, N., « La réforme de la Loi Informatique et libertés », dans *Revue française d'administration publique*, n 89, *La protection des données personnelles*, janvier-mars 1999, 46.

MISSIKA, J.-L. et FAIVRET, J.-P., « Informatique et Libertés », *Les temps modernes*, Septembre-Octobre 1977, 421.

OST, F., « Jupiter, Hercule, Hermès : trois modèles du juge », dans Pierre BOURETZ (dir.), *La force du droit*, Paris, Éditions Esprit, 1991, 263.

OST, F., « Le rôle du droit : de la vérité révélée à la réalité négociée », dans Gerard TIMSIT, Alain CLAISSE et Nicole BELLOUBET-FRIER (dir.), *Les administrations qui changent, Innovations techniques ou nouvelles logiques ?*, Paris, PUF, 1996, 73.

OST, F., « Le temps virtuel des lois post-modernes ou comment le droit se traite dans la société de l'information », dans Jean CLAM et Gilles MARTIN (dir.), *Les transformations de la régulation juridique*, Paris, L.G.D.J., 1988, 423.

PERELMAN, C., « Les notions à contenu variable, Essai de synthèse », dans Ch. PERELMAN et R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 363,1984.

POUND, R., « The Administrative Application of Legal Standards », *Reports of the American Bar Association*, vol. n.44, 1919, 445.

POULLET Y. et T. LÉONARD, « Les libertés comme fondement de la protection des données nominatives », dans François RIGAUX, *La vie privée, une liberté parmi les autres?*, Travaux de la Faculté de droit de Namur, t. 17, Bruxelles, Larcier, 1992.

POULLET, Y., « Réflexions introductives à propos du binôme Droit et sécurité », dans Joël HUBIN (dir.), *Sécurité informatique, entre technique et droit*, Cahiers du CRID, n° 14, Bruxelles, Story-Scientia, 1998, 185.

RIEDEL, E., « Standards and Sources. Farewell to the Exclusivity of the Sources Triad in International Law? » (1991) 2 *EJIL*, 58.

RIALS, S., « Les standards, notions critiques du droit », dans Ch. PERELMAN et R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Ch, Bruxelles, Bruylant, 1984.

RIGAUX, F., « La doctrine des droits de la personnalité », dans François RIGAUX (dir.), *La vie privée, une liberté parmi les autres ?*, Travaux de la Faculté de droit de Namur, t. 17, Bruxelles, Larcier, 1992, 116.

RIGAUX, F., « Le contrôle de la légitimité constitutionnelle ou internationale de la loi et des décisions judiciaires », dans François RIGAUX (dir.), *La vie privée, une liberté parmi les autres ?*, Travaux de la Faculté de droit de Namur, t. 17, Bruxelles, Larcier, 1992, 23.

RIGAUX, F., « Le droit entre un en déça et un au delà », dans François RIGAUX (dir.), *La vie privée, une liberté parmi les autres ?*, Travaux de la Faculté de droit de Namur, t. 17, Bruxelles, Larcier, 1992, 161.

RIGAUX, F., « Les paradoxes de la protection de la vie privée », dans Pierre TABATONI (dir.), *La protection de la vie privée dans la société de l'information*, Tome I, Paris, PUF, 2000, 9.

RIGAUX, F., « Libre circulation des données et protection de la vie privée dans l'espace européen », dans Pierre TABATONI (dir.), *La protection de la vie privée dans la société de l'information*, Tome II, Paris, PUF, 2000, 25.

ROBINSON, N., H. GRAUX, M. BOTTERMAN et L. VALERI, *Review of the European Data Protection Directive*, Sponsored by the Information Commissioner's Office, RAND Corporation, 2009.

ROCHER, G., « Pour une sociologie des ordres juridiques », *Les Cahiers de Droit*, vol. 29, nº 1, mars 1988, 116.

RODOTA, S., « Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives », *Mouvements des droits et des idées, « Sous contrôle, gouverner par les fichiers »*, nº 62, avril-juin 2010, 60.

SAURET, J., « Efficacité de l'administration électronique et service à l'administré : les enjeux de l'administration électronique », (2004) *Revue française d'administration publique* n 110, 279, 281.

SENDRA, A., « Informatique et Libertés : que change la réforme du 6 août 2004? », dans *Le harcèlement numérique*, Jean-Luc GIROT (dir.), Paris, Dalloz, 2005, 187.

SERWIN, A.B., « Privacy 3.0-The principle of proportionality », 42 *U. Mich. J.L. Reform* 869 2008-2009, 899.

SOLOVE, D.J., « A taxonomy of privacy », *University of Pennsylvania Law Review*, vol. 154, n° 3, Janvier 2006, 477.

SOLOVE D.J. et C. J. HOOFNAGLE, « A Model Regime of Privacy protection Version 2.0 », *GWU Law School Public Law Research Paper*, n° 132, avril 2005.

SOYER, J.-C., « L'avenir de la vie privée face aux effets pervers du progrès et de la vertu », dans Pierre TABATONI (dir.), *La protection de la vie privée dans la société de l'information*, T. 1, Paris, PUF, 2000, 7.

ST-AMANT, G., « E-Gouvernement : cadre d'évolution de l'administration électronique », (2005), *Revue Systèmes d'information et Management*, n° 1 vol. 10, 16.

TOLBERT, C.J., et K. MOSSBERGER, « The Effects of E-Government on Trust and Confidence in Government », 66 *Public Administration Review* (2006), vol. 66, n° 3, 354.

TRONC, J.-N., « L'administration et les technologies de l'information et de la communication » dans Danielle BAHU-LEYSER et Pascal FAURE (dir.), *Nouvelles technologies, nouvel État*, Paris, La Documentation Française, 1999, 151.

TRUDEL, P., « État de droit et e-gouvernement », dans Karim BENYEKHLEF et Pierre TRUDEL (DIR.), *État de droit et virtualité*, Montréal, Éditions Thémis, 2009, 373.

TRUDEL, P., « Gouvernance réseautique et effectivité des modes de protection des données personnelles dans les réseaux de cybersanté » dans Jean HERVEG (dir.), *La protection des données médicales, Les défis du XXI^e^ siècle*, Louvain-la-Neuve, Anthémis, 37.

TRUDEL, P., « Gouvernement électronique et interconnexion de fichiers administratifs dans l'État en réseau », *Revista Catalana de Dret Public*, n° 35, 2007, 247.

TRUDEL, P., « Hypothèses sur l'évolution des concepts du droit de la protection des données personnelles dans l'État en réseau », dans María Verónica PÉREZ-ASINARI et Pablo PALAZZI (dir.), *Défis du droit à la protection de la vie privée, Perspectives du droit européen et nord-américain*, Cahiers du CRID, nº 31, Bruxelles, Bruylant, 2008, 531.

TRUDEL, P., « Renforcer la protection de la vie privée dans l'État en réseau : l'aire de partage de données personnelles », (2004) *Revue française d'administration publique* n° 110, 257.

VALERO TORRIJOS, J. et M. FERNÁNDEZ SALMERÓN, « Protección de datos y Administración electrónica », *Revista Española de Protección de datos*, Juillet-Décembre 2006, I, 115.

WARREN, S.D., L.D. BRANDEIS, « The Right to Privacy », 4 Harv. L.Rev. 193 (1890).

WITHMAN, J. Q., « The two western Cultures of Privacy: Dignity versus Liberty », 113 Yale L.J. 1151 (2004), 1163.

WÜRTEMBERG, T. et G. SYDOW, « Administration électronique et vie privée en Allemagne », dans George CHATILLON et Bertrand DU MARAIS (dir.), *L'administration électronique au service des citoyens*, Bruxelles, Bruylant, 2003, 361.

***Thèses de doctorat et Mémoires de maîtrise***

BERTHOU, R., *L'évolution de la création du droit engendrée par Internet : vers un rôle de guide structurel pour l'ordre juridique européen*, thèse de doctorat, Rennes, Université de Rennes I, 2004.

BLANC-GONNET, P., *Protection de la vie privée et transparence à l'épreuve de l'informatique*, thèse de doctorat, Paris, Faculté de Droit de Saint Maur, Université Paris Val de Marne (Paris XII), 2001.

BOURGEOS, C., *L'anonymat et les nouvelles technologies de l'information*, thèse de doctorat, Paris, UFR de droit, Université Paris V, 2003.

DUASO CALÉS, R., *La protection des données personnelles contenues dans les documents accessibles sur Internet : le cas des données judiciaires*, mémoire de maîtrise, Montréal, Faculté de droit, Université de Montréal, 2002, en ligne : "https://papyrus.bib.umontreal.ca/jspui/bitstream/1866/2435/1/11449372.PDF" (consulté le 11 janvier 2011).

DUBUISSON, E., *La numérotation des personnes physiques*, thèse de doctorat, Paris, Faculté de droit, Université Paris XI, décembre 2004.

LESAULNIER, F., *L'information nominative*, thèse de doctorat, Faculté de droit, Paris, Économie-Sciences sociales, Université Panthéon-Assas, 2005.

LETTERON, R., *L'administré et le droit à l'information*, thèse de doctorat, Paris, UFR de Sciences juridiques, administratives et politiques, Université de Paris X, 1987.

VACARIE, I., *Le traitement informatique des données de santé*, thèse de doctorat, Paris, Université de Paris I, Panthéon-Sorbonne, 1988.

***Documents d'organismes publics***

**Commissariat à la protection de la vie privée du Canada**

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information sur les ÉFVP*, 2007, en ligne : "http://www.priv.gc.ca/fs-fi/02_05_d_33_f.cfm" (consulté le 7 juin 2011).

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche documentaire* : *Le suivi de l'enquête sur Facebook est terminé*, 22 septembre 2010, en ligne : "http://www.privcom.gc.ca/media/nr-c/2010/bg_100922_f.cfm (consulté le 20 mai 2011).

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Le dépistage génétique et la vie privée*, 1995.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Modifications immédiates proposées à l'égard de la Loi sur la protection des renseignements personnels*, Comparution devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, le 29 avril 2008.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Nos attentes : Un guide pour la présentation d'évaluations des facteurs relatifs à la vie privée au Commissariat à la protection de la vie privée du Canada*, mars 2011.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2000-2001 sur la Loi sur la protection des renseignements personnels*, 2001.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2004-2005 sur la Loi sur la protection des renseignements personnels*, 2005.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2005-2006 sur la Loi sur la protection des renseignements personnels*, 2006.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2006-2007, Rapport concernant la Loi sur la protection des renseignements personnels*, 2007.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2008-2009 concernant la Loi sur la protection des renseignements personnels*, 2009.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2008 sur la Loi sur la protection des renseignements personnels et les documents électroniques*, 2009.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport de vérification des pratiques de gestion des renseignements personnels de l'Agence des services transfrontaliers du Canada*, Juin 2006.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Responsabilité du gouvernement en matière de renseignements personnels ; Réforme de la Loi sur la protection des renseignements personnels, juin 2006.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Une question de confiance : Intégrer le droit à la vie privée aux mesures de sécurité publique au 21e siècle*, Document de référence, Novembre 2010.

**Commission nationale de l'informatique et des libertés**

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Avis sur le Projet de Loi modifiant la Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, 26 septembre 2000.

COMMISSION INFORMATIQUE ET LIBERTÉS, *Rapport de la Commission Informatique et Libertés*, Paris, La Documentation Française, 1975.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Rapport de la Commission Nationale de l'Informatique et des Libertés, Bilan et perspectives, 1978-1980*, Paris, La Documentation Française, 1980.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *2e Rapport d'activité de la Commission Nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1981.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *3e Rapport d'activité de la Commission Nationale de l'Informatique et des libertés*, Paris, La Documentation Française, 1982.

COMMISION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *4e Rapport d'activité de la Commission nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1983.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *6e Rapport d'activité de la Commission nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1985.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *10e Rapport d'activité de la Commission nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1989.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *11e Rapport d'activité de la Commission nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1990.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *15e Rapport d'activité de la Commission nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1994.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *16e Rapport d'activité de la Commission nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1995.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *19e Rapport d'activité de la Commission nationale de l'informatique et des libertés*, Paris, La Documentation Française, 1999.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *20e Rapport d'activité de la Commission nationale de l'informatique et des libertés*, Paris, La Documentation Française, 2000.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *22e Rapport d'activité*, 2001 *de la Commission nationale de l'informatique et des libertés*, en ligne : "http://www.cnil.fr" (consulté le 12 février 2011).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *24e Rapport d'activité de la Commission nationale de l'informatique et des libertés*, 2003, en ligne : "http://www.cnil.fr/" (consulté le 11 février 2010).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *20e Rapport d'activité de la Commission nationale de l'informatique et des libertés*, Paris, La Documentation française, Paris, 2009.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *30e Rapport d'activité de la Commission Nationale de l'Informatique et des Libertés*, Paris, La Documentation Française, 2009.

**Secrétariat du Conseil du Trésor**

SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Directive sur l'évaluation des facteurs relatifs à la vie privée*, 1er avril 2010, en ligne : "http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=18308" (consulté le 10 juillet 2011).

SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Politique sur la protection de la vie privée*, 2008, en ligne : "http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510" (consulté le 20 octobre 2010).

SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Politique d'évaluation des facteurs relatifs à la vie privée*, 2002, en ligne : "http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12450" (consulté le 11 février 2011).

SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Politique sur le couplage des données*, 1989.

SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Rapports annuels sur la Loi sur l'accès à l'information et la Loi sur la protection des renseignements personnels - Rapport de mise en œuvre n 109*, en ligne : "http://www.tbs-sct.gc.ca/atip-aiprp/impl-rep/2008/109-imp-mise-fra.asp" (consulté le 3 décembre 2010).

SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Usage et communication de renseignements personnels*, 1993, en ligne : "http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/CHAP2_4-2-fra.asp" (consulté le 13 novembre 2010).

**Autres organismes publics**

**Canada**

BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA, *Rapport de mai 2008 sur Rapport de la vérificatrice générale du Canada - Chapitre 5 - La surveillance des maladies infectieuses*.

GOUVERNEMENT DU CANADA, *Accès et renseignements personnels : les prochaines étapes*, 1987.

STANDING COMITTEE ON JUSTICE AND SOLLICITOR GENERAL ON THE REVIEW OF THE ACCESS TO INFORMATION ACT AND THE PRIVACY ACT,

*Une question à deux volets : Comment améliorer le droit d'accès à l'information tout en renforçant les mesures de protection des renseignements personnels*, 1987.

**France**

SECRÉTARIAT D'ÉTAT AUPRÈS DU PREMIER MINISTRE CHARGÉ DE LA FONCTION PUBLIQUE ET DES SIMPLIFICATIONS ADMINISTRATIVES, *La mutation de l'administration, objectifs et conditions*, Paris, La Documentation Française, 1986.

SERVICE AUX AFFAIRES EUROPÉENNES, SÉNAT FRANÇAIS, *L'interconnexion des fichiers administratifs*, Juin 1999.

**Ontario**

COMMISSAIRE À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE L'ONTARIO, *Perspectives*, vol. 5, n° 2, Printemps 2006.

**Québec**

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Une réforme de l'accès à l'information : le choix de la transparence, Rapport sur la mise en œuvre de la Loi sur l'accès et de la Loi sur le secteur privé*, Novembre 2002.

**Union européenne**

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL, CONSEIL DE L'EUROPE, *Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques*, février 2005.

COMMISSION EUROPÉENNE, *Décision de la Commission du 20 décembre 2001 constatant, conformément à la Directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, (JO L 2 du 4.1.2002, p. 13–16).*

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS, *Une approche globale de la protection des données à caractère personnel dans l'Union européenne*, Bruxelles, le 4 novembre 2010.

CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel du 28 janvier 1981 du Conseil de l'Europe*, en ligne : "http://conventions.coe.int/Treaty/FR/Reports/Html/108.htm" (consulté le 20 octobre 2010).

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, *Communiqué de presse sur la « Stratégie de réforme de la protection des données : le CEPC présente sa conception du nouveau cadre juridique »*, Bruxelles, mardi 18 janvier 2011.

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament. The Council, the Economic and Social Committee and the Committee of the Regions – « A comprehensive approach on personal data protection in the European Union »*, 14 janvier 2011.

GROUPE « ARTICLE 29 », *Avis 2/2001 sur le niveau de protection garanti par la Loi canadienne sur la protection des renseignements personnels et les documents électroniques*, 2001.

GROUPE DE TRAVAIL « ARTICLE 29 », *Avis nº 3/2010 sur le principe de responsabilité*, adopté le 13 juillet 2010.

GROUPE DE TRAVAIL « ARTICLE 29 » ET GROUPE DE TRAVAIL « POLICE ET JUSTICE », *L'avenir de la protection de la vie privée*, Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, adoptée le 1er décembre 2009.

GROUPE « ARTICLE 29 » SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES, *Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la Directive communautaire sur la protection des données*, GT 12, 1998.

***Autres documents***

32ND INTERNATIONAL PRIVACY OF DATA PROTECTION AND PRIVACY COMMISSIONERS, *Privacy by Design Resolution*, 27-29 Octobre 2010, Jerusalem, Israel, en ligne: www. privacybydesign.ca (consulté le 12 mars 2011).

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) et PRIVACY INTERNATIONAL (PI), *Privacy and Human Rights 2004, An International Survey of Privacy Laws an Developments*, 2004.

*Éthique publique, Revue internationale d'éthique sociétale et gouvernementale*, « Les enjeux éthiques de la gestion de l'information », automne 2004, vol. 6, n° 2, Éditions Liber, Montréal, Québec, 2004.

FLAHERTY, D. H., *Réflexions sur la réforme de la Loi sur la protection des renseignements personnels*, Juin 2008, en ligne : "http://www.priv.gc.ca/information/pub/pa_ref_df_f.pdf" (consulté le 13 mars 2011).

FORUM DES DROITS SUR L'INTERNET, *Conclusions dur le débat public « Administration publique et données personnelles »*, 2002, en ligne : "http://www.foruminternet.org/publications/lire.phtml?id=476" (consulté le 15 avril 2010).

FORUM DES DROITS SUR L'INTERNET, *Recommandation sur le développement de l'administration électronique*, février 2003, en ligne : "http://www.foruminternet.org/recommandations/lire.phtml?id=493" (consulté le 14 avril 2010).

INSTITUT DES SERVICES AXÉS SUR LES CITOYENS, *Ententes d'échange de renseignements personnels, Lignes directrices sur les pratiques exemplaires*, p. 36, en ligne :
http://www.iccs- isac.org/fr/practice/privacy.html (consulté le 15 mai 2011).

REIDENBERG, J.R. et P. M. SCHWARTZ, *Data protection law and on-line services : regulatory responses*, Étude préparé dans le cadre du projet « Vie privée et société de l'information : Étude sur les problèmes posés par les nouveaux services en ligne en matière de protection des données et de la vie privée », commandé à ARETE par la DG XV de la Commission Européenne, Bruxelles, 1998.

TRUDEL, P. et F. ABRAN, *Analysis of the Adequacy of Personal Data Protection in Canada, Report presented at the request of the European Commission, Justice and Home Affairs DG*, 2005.

TRUDEL, P., K. BENYEKHLEF, F. ABRAN, C. CHASSIGNEUX, R. DUASO CALÉS et R. LANGELIER, *Guide pour maîtriser les risques juridiques des cyberconsultations*, Document préparé pour le Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles du Secrétariat du Conseil du Trésor et le Groupe de travail sur la Cyberdémocratie, Gouvernement du Québec, Novembre 2004.

TRUDEL, P., *Normativités en réseau et gestions des risques par les états et les usagers d'Internet*, Analyse réalisé dans le cadre d'un programme de recherche sur les méthodes de régulation des médias dans la nouvelle économie financée en partie par le Groupe TVA en vertu d'une contribution versée dans le cadre du programme des avantages tangibles mis en place lors de la transaction par laquelle Québécor Media a acquis le contrôle de TVA.

***Présentations et allocutions dans le cadre de conférences***

BLACK, H., *Réforme des lois sur la protection des renseignements personnels et de la vie privée : Réponse à un monde en réseau*, Allocution présentée dans la Série Conférenciers invités McCarthy Tétrault, Halifax (Nouvelle-Écosse), 3 février 2005.

BOURCIER, D., *Les allemands et les Français face à la vie privée, que nous apprend le droit sur les cultures?*, Actes du 41e Congrès du Mouvement du jeune notariat, du 6 au 10 octobre 2010.

BOURCIER, D., *Sciences du droit, complexité, serendipité*, Exposé dans le cadre de l'Atelier Complexité et Politiques Publiques, 23-24 septembre 2010, en ligne : "http://complexitejuridique.files.wordpress.com/2010/09/atelier-complexite-droitcomplexite-serendipite4.ppt" \l "1" (consulté le 2 février 2011).

BOURCIER, D., *Sciences juridiques, complexité, serendipité*, Résumé de l'exposé dans le cadre de l'Atelier Complexité et Politiques Publiques, 23-24 septembre 2010.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Équilibre entre protection de la vie privée et circulation de l'information*, Allocution présentée par Patricia KOSSEIM dans le cadre du Forum organisé par le *Population Therapeutics Research Group*, St. John's, Terre-Neuve-et-Labrador, novembre 2007.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La protection de la vie privée à l'ère du gouvernement 2.0*, Commentaires présentés par Jennifer STODDART à l'occasion du Salon des gouvernements innovateurs du Canada 2010 « Les gouvernements hautement performants », le 7 octobre 2010, Ottawa, Ontario.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Leçons tirées du secteur public*, Comentaires présentés par Chantal BERNIER dans le cadre d'un débat d'experts lors de la Conférence du groupe *Access Privacy*, le 25 mars 2010, Toronto, Ontario.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Reconstruire la Loi sur la protection des renseignements personnels*, Allocution présentée par Jennifer STODDART au Colloque organisé par Riley Information Systems, 21 février 2007, Ottawa.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Règlement fédéral sur la protection des renseignements personnels en 2010 : le bilan*, Commentaires présentés par Patricia KOSSEIM à l'occasion de la 6e conférence annuelle de FJP sur le droit administratif organisée par Osgoode Law School, le 19 octobre 2010, Toronto, Ontario, en ligne : "http://www.priv.gc.ca/speech/2010/sp-d_20101019_pk_f.cfm"

COMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Allocution présentée par C. BEAULÉ au *Groupe de travail interministériel sur la vie privée et le Gouvernement en direct*, Ottawa, Ontario, 8 mai 2002, en ligne : "http://www.priv.gc.ca/speech/02_05_a_020508_f.cfm" (consulté le 14 mai 2011).

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, « New European rules on data protection », Conférence prononcée par Peter HUSTINX au *Joint High Level Meeting on Data Protection Day, Organised by the European Commission and the Council of Europe*, Bruxelles, le 28 janvier 2011.

DE ROY, D., C. DE TEWARGNE et Y. POULLET, *La Convention européenne des droits de l'homme en filigrane de l'administration électronique*, version mise à jour d'une présentation orale au colloque sur « Cinquante ans d'application de la CEDH en Belgique : entre ombres et lumières », organisé par le Centre de recherche en droit public de l'ULB, les 20 et 21 octobre 2005 à Bruxelles, en ligne : "http://www.crid.be/" (consulté le 3 avril 2011).

FERNÁNDEZ SALMERÓN, M., *La cesión de datos personales en las Administraciones Públicas. Distinción de figuras afines*, Texte de l'allocution dans le cadre de la conférence organisée à l'*Agencia Catalana de Protección de datos*, Barcelona, 25 mai de 2004.

GAUTRAIS, V., *Fictions et présomptions : outils juridiques d'intégration des technologies*, Présentation dans le cadre de la Conférence « Sécurité juridique et sécurité technique : indépendance ou métissage » organisée par le Programme international de coopération scientifique (CRDP / CECOJI), Montréal, 30 septembre 2003, en ligne : "http://www.lex-electronica.org/docs/articles_105.pdf" (consulté le 14 décembre 2010).

*Internet, la révolution numérique crée-t-elle une révolution juridique ?*, 1res Rencontres parlementaires sur la Société de l'information et l'Internet, à l'initiative de Christian PAUL, Paris, Éd. M & M Conseil, 1999.

LENK, K., *Innovation Impact Assessment : une procédure pour évaluer ex ante la complexité de la mise en oeuvre d'une politique publique*, Présentation dans le cadre de l'Atelier Complexité et Politiques Publiques, tenu à Paris les 23 et 24 septembre 2010, en ligne : "http://complexitejuridique.files.wordpress.com/2010/09/lenk_complex.ppt" (consulté le 14 mai 2011).

LÉONARD, T., *Conversations cridiennes autour du principe de finalité*, présentation dans le cadre de la Conférence des 30 ans du CRID, Namur, Belgique, le 22 janvier 2010.

POULLET, Y., « Cloud Computing and Privacy Issues – first reflections », Présentation lors du Séminaire « Privacy and Security », organisé par *l'Agencia Española de protección de datos* dans le cadre du Projet « Vie Privée et Sécurité », Madrid, 8 juin 2010.

POULLET, Y., *Le cyberespace v.(?) la vie privée*, Conférence dans le cadre du Séminaire international « État de droit et virtualité », Montréal, les 23 et 24 octobre 2007, en ligne : "http://www.etatdedroitetvirtualite.net/videos.html" (consulté le 20 mai 2011).

TRUDEL, P., *État de droit et effectivité de la protection de la vie privée dans les réseaux du e-gouvernement*, Communication présentée lors du colloque national « Technologies, vie privée et justice », tenu à Toronto par l'Institut canadien d'administration de la justice (ICAJ) du 28 au 30 septembre 2005,
p. 13, en ligne : "http://www.chairelrwilson.ca" (consulté le 12 mars 2011).

***Articles de journaux***

BOUCHER, P., « *Safari* ou la chasse aux français », *Le Monde*, 21 mars 1974.

CHRISTENSEN, M., « Facebook is watching you », *Le Monde diplomatique, Manière de voir, Internet, révolution culturelle*, 109, février-mars 2010, 52.

LE CROSNIER, H., « À l'ère de l'informatique en nuages », *Le Monde diplomatique, Manière de voir, Internet, révolution culturelle*, no. 109, 109, février-mars 2010, 74.

MITJANS i PERELLÓ, E., « Ultimátum a Facebook », *La Vanguardia*, jeudi 13 août 2009.

STELTER, B., « Upending anonymity, these days the web unmasks everyone », *The New York Times*, 20 juin 2011, en ligne :
"http://www.nytimes.com/2011/06/21/us/21anonymity.html?_r=2&hp" (consulté le 2 août 2011).

***Autres documents***

*Compte-rendu du débat à l'Assemblée Nationale de la Première séance du 4 octobre 1977.*

*Compte rendu du débat au Sénat français de la Séance du 17 novembre 1977.*

*Extraits des débats au Sénat*, première lecture de la Loi Informatique et Libertés modifiée, Séance publique du 1er avril 2003.

*Extraits des débats à l'Assemblée nationale,* deuxième lecture de la Loi Informatique et Libertés modifiée, Séance publique du 29 avril 2004.

*Extraits des débats au Sénat*, deuxième lecture de la Loi Informatique et Libertés modifiée, Débats en séance publique du 15 juillet 2004.

*Extraits du Rapport nº 218 de M. Alex Türk.* Sénat, première lecture de la Loi Informatique et Libertés modifiée

*Extraits du Rapport nº 367 de M. Alex Türk.* Sénat, deuxième lecture de la Loi Informatique et Libertés modifiée.

*Extraits du Rapport nº 1537 de M. Francis Delattre.* Assemblée Nationale, deuxième lecture de la Loi I et L modifiée.

*Rapport de M. FOYER, au nom de la commission des lois : Doc. Ass. Nat. n. 3125 du 4-10-1977.*

*Rapport de M. J. THYRAUD, au nom de la commission des lois : Doc. Sénat n. 72 du 10-11-1977.*