Chaire L.R. Wilson
sur le droit des technologies
de l'information et du
commerce électronique

CENTRE DE
RECHERCHE EN
DROIT PUBLIC
FACULTE DE DROIT
UNIVERSITE DE MONTREAL

Guide pour l'élaboration d'une politique de confidentialité

Par

Cynthia CHASSIGNEUX

Juin 2008

Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique
Centre de recherche en droit public
Faculté de droit
Université de Montréal
C. P. 6128, succ. Centre-ville
Montréal (Québec)
H3C 3J7

ISBN : 978-2-922112-03-0 (PDF)

Cette publication est accessible sur le site de la *Chaire L.R. Wilson* : http://www.chairelrwilson.ca

Avant-propos

Le présent document s'inscrit dans le cadre d'une recherche post-doctorale réalisée grâce au soutien, d'une part, du *Centre de recherche en éthique de l'Université de Montréal* (CRÉUM – Bourse 2005-2006) et, d'autre part, de la *Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique* (Bourse 2007-2008).

Cette recherche a pour objectif d'examiner les mécanismes de production de la confiance dans les environnements électroniques. En effet, du fait de la dématérialisation de l'environnement et des voies offertes quant à la surveillance des actions des internautes tant dans leur vie professionnelle que quotidienne, la problématique de la protection de la vie privée est relancée. Non pas que cette question ait perdu de son intérêt au cours des dernières années. Toutefois, le développement d'Internet cristallise, d'une certaine manière, les craintes longtemps associées à l'informatisation des activités humaines.

Les possibilités techniques des environnements électroniques augmentent considérablement la masse d'informations et, par conséquent, de renseignements personnels circulant sur le réseau. Cette situation suscite dès lors une série d'interrogations légitimes quant aux moyens susceptibles de protéger la vie privée et, plus particulièrement les données qui concernent une personne physique et permettent de l'identifier.

Ces interrogations nécessitent de s'intéresser à l'encadrement juridique du traitement des renseignements personnels sur Internet. Cependant, les environnements électroniques modifiant les perceptions traditionnelles du droit, il n'est plus possible d'envisager la compréhension du cadre juridique d'une activité selon une vision linéaire. Il est alors important de prendre en considération d'autres normes qui ne sont pas élaborées par la puissance publique, mais qui ont néanmoins un effet normatif incontestable. Cette situation a comme corollaire, d'une part, de redéfinir l'espace dans lequel circulent les renseignements personnels et, d'autre part, de revoir les instruments normatifs, étatiques et non étatiques, qui tout en permettant leur protection encadrent leur communication.

Par conséquent, la protection des renseignements personnels ne pouvant plus s'envisager sous le seul angle du droit étatique du fait du caractère intangible ou encore transfrontalier d'Internet, certains instruments issus de l'autorégulation visant à encadrer les activités en ligne doivent être pris en considération. Ces outils reprennent les principes visant à encourager la transparence quant à la collecte et à l'utilisation des renseignements personnels tant de la part des organismes publics que des entreprises.

Cette transparence vise à favoriser l'établissement d'un sentiment de confiance chez les citoyens-internautes, sentiment nécessaire à la bonne gestion des environnements électroniques. Ce souci de transparence oblige les organismes publics et les entreprises à préciser, entre autres, quels sont les renseignements qui seront collectés, quel est l'usage qui en sera fait, qui y aura accès, quelles sont les mesures de sécurité prises pour en assurer la confidentialité, comment la personne concernée pourra exercer son droit d'accès ou de rectification et, le cas échéant porter plainte en cas de manquement. Ce devoir d'information du destinataire de la confiance est nécessaire pour permettre une forme d'abandon de la part de l'émetteur de celle-ci.

Cette référence à la notion de confiance et à son rôle quant au choix d'un citoyen-internaute à entrer en relation avec un organisme public ou une entreprise en particulier montre l'importance de cette notion dans le développement des activités en ligne.

Partant, nous nous sommes intéressés, dans un premier temps, aux mécanismes de production de la confiance dans les environnements électroniques. Nous avons alors envisagés les fondements définitionnels et les catégorisations possibles de la confiance[1].

Dans un deuxième temps, nous avons pris en considération les politiques de confidentialité formalisant les engagements des destinataires de la confiance en ce qui a trait à la protection des renseignements personnels des émetteurs de la confiance[2].

L'analyse de leurs spécificités, de leur contenu et de leur mise en œuvre nous a permis d'établir, dans un troisième temps, un guide visant à sensibiliser les acteurs des environnements électroniques sur le besoin de renforcer le sentiment de confiance nécessaire au bon déroulement des activités effectuées de tels environnements. En effet, même si les politiques de confidentialité ne produisent pas les effets escomptés, nous sommes d'avis qu'elles sont néanmoins susceptibles d'établir un lien de confiance entre l'émetteur et le destinataire de cette dernière.

---

1 Cynthia CHASSIGNEUX, « La confiance, instrument de régulation des environnements électroniques », (2007) 37 *Revue de droit de l'Université de Sherbrooke* 441, également disponible à l'adresse suivante : http://hdl.handle.net/1866/2252.

2 Cynthia CHASSIGNEUX, « Pour une analyse de l'effectivité des politiques de confidentialité », (2008) *Communication-Commerce électronique* (à paraître en septembre 2008).

Introduction

Que l'on considère les dispositions légales ou les recommandations émises par différentes autorités de contrôle, au Canada, en Europe ou encore aux Etats-Unis, force est de constater l'importance accordée à la communication par la partie la plus forte au contrat d'informations susceptibles d'intéresser l'autre partie. L'obligation d'information caractérise cette idée : information quant au prix, quant aux caractéristiques du bien et/ou du service, quant au traitement des renseignements personnels.

En ce qui a trait à ce dernier élément, cette obligation s'entend du fait pour toute entité juridique, publique ou privée, qui entend collecter des renseignements permettant d'identifier, directement ou indirectement, une personne physique, d'informer préalablement la personne concernée sur certains points. Ainsi, devront notamment être précisé quels sont les renseignements qui seront collectés, quel est l'usage qui en sera fait, qui y aura accès, quelles sont les mesures de sécurité prises pour en assurer la confidentialité, comment la personne concernée pourra exercer son droit d'accès ou de rectification et, le cas échéant porter plainte en cas de manquement. Cette information doit être claire, compréhensible et facilement accessible[1]. Dans les environnements électroniques, elle sera contenue dans les politiques de confidentialité formalisant les engagements des gestionnaires quant aux renseignements personnels collectés sur un site Web.

Cette transparence vise à favoriser l'établissement d'un sentiment de confiance entre un organisme public ou ministère et un citoyen, entre une entreprise privée et un client, par exemple. Ce sentiment, devant prévaloir à toute relation, peu importe sa nature, est indispensable dans un environnement où les parties ne sont pas en présence l'une de l'autre, ne sont pas sur le même territoire.

Dans cette optique d'information et de transparence, le présent guide expose quelles sont les exigences devant être prises en considération lors de l'élaboration d'une politique de confidentialité. Dès lors, d'une part, sont décrites les qualités que doivent renfermer une telle politique et, d'autre part, sont analysés les enjeux inhérents à chacune de ses composantes. Une foire aux questions sur les tenants et les

---

1 Selon Boulanger et de Terwangue, cette transparence permet « à chaque individu de savoir qui sait quoi sur lui et pour en faire quoi. C'est à cette seule condition de connaissance que peut s'exercer la maîtrise par chacun du sort réservé aux informations qui le concernent, à son « image informationnelle » », Marie-Hélène BOULANGER et Cécile de TERWANGUE, « Internet et le respect de la vie privée », dans Étienne MONTERO, *Internet face au droit*, Namur, C.R.I.D., 1997, pp. 190-213, à la page 204.

aboutissants des politiques de confidentialité est également proposée. Enfin, une grille de vérification est présentée.

A. L'objectif du guide

Le présent guide vise à procurer un outil à l'intention des organismes publics ou ministères et des entreprises privées oeuvrant dans un environnement électronique (ci-après « les gestionnaires d'environnements électroniques » ou « gestionnaires ») lors de l'élaboration de leur politique de confidentialité. Cet outil leur fournira les éclairages nécessaires afin de prendre les mesures adéquates afin que la collecte et le traitement des renseignements personnels se déroulent dans le respect des principes reconnus en ce domaine.

B. Les destinataires du guide

Ce guide s'adresse à toutes personnes, plus particulièrement aux gestionnaires d'environnements électroniques, qui entendent collecter, directement ou indirectement, et utiliser des renseignements personnels, c'est-à-dire tout renseignement permettant d'identifier une personne physique. Ce guide vise à documenter les gestionnaires quant aux enjeux de la protection des renseignements personnels en leur indiquant les éléments devant être pris en considération lors de l'élaboration d'une politique de confidentialité.

C. La portée du guide

Ce guide se veut didactique. Il vise à présenter les qualités des politiques de confidentialité. Il vise également à dresser un portrait des étapes conduisant à l'élaboration de ces politiques, étapes tenant compte des obligations incombant aux gestionnaires d'environnements électroniques au regard des principes de protection et du cycle de renseignements personnels. Il vise aussi à établir une foire aux questions permettant de répondre aux interrogations les plus fréquemment posées. Il vise enfin à proposer une grille de vérification. Il convient néanmoins de préciser que les recommandations que peut contenir ce guide sont de portée générale et ne sauraient remplacer une expertise spécifique dans des cas particuliers.

I. Les principales qualités d'une politique de confidentialité

La transparence des activités en ligne doit conduire les gestionnaires d'environnements électroniques à tout mettre en œuvre pour permettre aux internautes de prendre connaissance des engagements contenus dans les politiques de confidentialité. Dès lors, en écho aux recommandations faites par Nielsen sur la façon de présenter une information sur un support électronique[2], ces politiques doivent – utiliser un langage simple, direct et sans ambiguïté – contenir des informations pertinentes au regard de l'activité considérée – être concises – être structurées de façon à rendre l'information accessible.

A. Clarté

La clarté s'entend comme étant le « caractère de ce qui est facilement intelligible »[3]. Cette clarté est signe de connaissance : connaissance du domaine dans lequel on entend évoluer, de ses droits et de ses obligations, connaissance des outils de communication permettant de diffuser l'information.

Partant, même si « des études montrent que bon nombre de notices d'information sur la protection de la vie privée sont trop longues, déconcertantes et émaillées de formulations juridiques compliquées »[4], il est important d'insister sur la « nécessité de présenter des informations avec un contenu cohérent et approprié à la situation de la collecte des données »[5]. En effet, trop d'information tue l'information[6]. En effet,

---

2 Jacob NIELSEN, *Writing for the Web,* http://www.sun.com/ 980713/webwriting. Voir également, FEDERAL TRADE COMMISSION, *Getting Noticed : Writing Effective Financial Privacy Notices*, octobre 2002, http://www.ftc.gov/bcp/conline/pubs/buspubs/getnoticed.shtm.

3 *Le Petit Robert*.

4 ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Simplifier les notices d'information sur la protection de la vie privée : rapport et recommandations de l'OCDE*, 24 juillet 2006, DSTI/ICCP/REG(2006)5/FINAL, p. 2.

5 GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis sur « Dispositions davantage harmonisées en matière d'informations » »*, WP 100, 25 novembre 2004, p. 5.

6 Selon Abrams et Crompton, « privacy noices are the windows to how organisations collect, use, share and protect the information that pertains to individuals. As information processes have become more complex, privacy notices have become very long, mirroring this complexity. The effect has been to obscure the content that individuals need to know when making judgments about with whom they will do business. The lack of clarity has been an impediment to online commerce », Marty ABRAMS and Malcolm CROMPTON, « Multi-layered privacy notices – a better way », (2005) 2-1 *Privacy Law Bulletin* 1, 1.

> *[la] compréhension par les personnes concernées est un objectif important afin que ces dernières puissent prendre des décisions informées et qu'elles possèdent un niveau de connaissance et de compréhension suffisant pour influencer les pratiques des responsables du traitement des données. Dans ce contexte, il est important de veiller à ce que l'information soit communiquée de manière appropriée aux personnes ayant des besoins particuliers (par exemple, aux enfants)*.[7]

C'est pourquoi, les gestionnaires doivent indiquer leurs intentions en matière de renseignements personnels « sous une forme généralement compréhensible »[8].

Ce souci de clarté n'est pas sans rappeler les propos de Gautrais et Mackaay indiquant que

> *[l]e juriste qui élabore le contrat à destination d'Internet, plutôt que de simplement « scanner » le contrat existant, aurait donc intérêt à observer des consignes comme les suivantes : un texte plus court, ne nécessitant pas ou peu de défilement; une utilisation de phrases simples; l'utilisation d'un plan; l'utilisation de puces pour bien distinguer les éléments importants; l'utilisation de caractères gras, voire de majuscule, pour mettre en exergue les points saillants; l'utilisation modérée et contrôlée des liens hypertextes; le bannissement de pratiques qui pourraient occasionner des doutes ou de l'inconfort auprès de l'adhérent comme le « framing » ou les sites qui bloquent le retour en arrière, etc.*[9]

Clarté des intentions, clarté dans la présentation de celles-ci, tout ceci conduit les gestionnaires d'environnements électroniques, d'une part, à réfléchir sur les raisons de la collecte, sur les finalités du traitement, sur leur responsabilité et, d'autre part, à présenter cette information de façon concise.

---

7 GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, op. cit., note 4, p. 7 et 8.

8 Loi sur la protection des renseignements personnels et les documents électroniques, L. C. 2000, c. 5, art. 4.8.1 Annexe 1. (ci-après « LPRPDÉ »).

9 Vincent GAUTRAIS et Ejan MACKAAY, « Les contrats informatiques », dans Denys-Claude LAMONTAGNE (dir.), Droit spécialisé des contrats. Les contrats relatifs à l'entreprise, Cowansville, Éditions Yvon Blais, 2001, pp. 279 à 315, à la page 297.

À retenir
• Formuler vos intentions en termes simples, intelligibles par tout un chacun. • Utiliser des phrases courtes. Ne pas diluer l'information. • Faites ressortir l'information essentielle (quels sont les renseignements personnels qui seront collectés, pourquoi, pour qui, qui est responsable de la gestion des renseignements et de la PRP, comment exercer le droit d'accès).

B. Concision

La concision s'entend de ce « qui s'exprime, pour un contenu donné, en peu de mots »[10]. Cette volonté de concision s'illustre par le recours grandissant aux politiques multistrates (ou *multi-layered privacy notices*), c'est-à-dire des politiques dont les informations sont présentées sous une forme condensée et, si l'internaute souhaite obtenir plus de détails, il lui est loisible de cliquer sur un lien lui donnant accès à une information complète. Par conséquent, après avoir déterminé quels sont les renseignements nécessaires à la réalisation de l'objet du traitement, il est recommandé aux gestionnaires d'environnements électroniques d'établir une politique de confidentialité complète, une condensée et une courte[11].

Cette méthode, préconisée, en 2001, par le *Center for Information Policy Leadership*, est largement approuvée par les autorités nationales et internationales. Ainsi, lors d'un atelier qui s'est tenu à Berlin, au lendemain de la 25ème conférence internationale des commissaires à la protection des données et de la vie privée, les participants ont adopté la résolution suivante :

> ***Multi-layered*** *: Privacy information cannot and should not normally be conveyed in a single document or message. Instead, information about an organization's privacy practices should be provided in a layered format. The "short" (condensed or highlights) layer should provide, in a highly readable format, the most important*

10 *Le Petit Robert*.

11 THE CENTER FOR INFORMATION POLICY LEADERSHIP, *Ten steps to develop a multilayered privacy notice*, 2001. Il est indiqué que « creating a privacy notice should not be viewed as an intimidating process. Developing a multilayered notice is no more difficult than a full legally compliant notice », p. 4. Dès lors, les entreprises doivent respecter les 10 étapes suivantes : 1) Determine what your company does with personal data; 2) Determine whether your company's treatment of personal data is legally compliant; 3) Develop and test an internal privacy policy that reflects how your company treats personal data; 4) Use that internal policy to create the organization's complete external privacy policy; 5) Test and revise the full privacy notice; 6) Create the condensed notice; 7) Harmonize the full and condensed notices together; 8) Create the short notice; 9) Review and test the multilayered notices; 10) Publish your new multilayered notice. Ces étapes sont développées aux pp. 4 et suiv. .

> *information that individuals need to understand their position and make decisions. Even shorter notice layers may be acceptable for coupons, mobile phone screens, and other places where notice is needed, but space is extremely limited. Additional information should then be easily accessible in longer, more complete layers. This approach improves both comprehension and legal compliance, because the privacy notice – the whole framework - can deliver content in a more understandable fashion, and in a manner appropriate to the medium and the targeted audience.* [12]

Cette façon d'envisager la présentation des politiques de confidentialité est réaffirmée dans un avis du *Groupe 29 sur la protection des données*, dans les termes suivants :

> **Soutien du concept d'un format multistrates pour les avis aux personnes concernées**. *Les avis multistrates peuvent contribuer à améliorer la qualité des informations sur la protection des données reçues en focalisant chaque strate sur les informations dont la personne a besoin pour comprendre sa position et prendre des décisions. Lorsque l'espace / le temps de communication est limité, les formats multistrates peuvent améliorer la lisibilité des avis.* [13]

Elle l'est également dans un récent rapport de l'Organisation de Coopération et de Développement Économiques encourageant les gestionnaires d'environnements électroniques à préparer une déclaration complète[14], à élaborer une notice simplifiée et à publier cette dernière « en bonne place sur le site Internet (…) afin que tout personne dont [une] organisation peut être amenée à utiliser des données personnelles puisse y accéder et la lire rapidement et aisément »[15].

---

12 *Berlin Privacy Notices Memorandum*, 2004.

13 GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *op. cit.*, note 5, p. 8.

14 Dans cette déclaration, la personne concernée doit retrouver une description détaillée de la politique et des pratiques du site Web, description faisant écho aux exigences énoncées notamment à l'article 4.8.2 Annexe 1 LPRPDÉ ; à l'article 65 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, LRQ c. A-2.1 (ci-après « Loi sur l'accès ») ; à l'article 8 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, LRQ, c. P-39.1 (ci-après « LPRPSP ») ; aux articles 10 et 11 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*, JO L 281 du 23.11.1995, pp. 31 à 50 (ci-après « Directive 95/46/CE ») ; à la section « notice » des Safe Harbor Principles, http://www.export.gov/safeharbor. .

15 ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *op. cit.*, note 4, p. 7.

À retenir

• Préparer deux politiques de confidentialité : une longue et une abrégée.
  • La version longue doit contenir tous les éléments vous permettant de répondre à l'ensemble de vos obligations en matière de protection des renseignements personnels.
  • La version abrégée doit contenir les éléments essentiels de vos engagements et, diriger vers la version longue.
• Utiliser des phrases courtes. Ne pas diluer l'information.

C. Accessibilité

L'accessibilité s'entend comme étant le fait de pouvoir prendre connaissance de quelque chose sans obstacle. Le fait de rendre difficile l'accès à l'information peut nuire au lien de confiance entre le destinataire et l'émetteur de celle-ci. En effet, même si les conditions d'utilisation d'un site Web ou la politique de confidentialité ne sont pas forcément lues par les internautes, cette information doit être disponible en tout temps. L'internaute doit pouvoir s'y référer sans difficulté[16]. C'est pourquoi, il est recommandé aux gestionnaires d'environnements électroniques de « faire en sorte que des renseignements précis sur [leurs] politiques et [leurs] pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne »[17].

À retenir
• Faire en sorte que la politique de confidentialité soit facilement accessible, à toute personne, en tout temps. • Accessibilité = un clic

16 Yves POULLET, « Mieux sensibiliser les personnes concernées, les rendre acteurs de leur propre protection », (2005) 5 *Revue Lamy – Droit de l'immatériel* 47-57. Dans cet article, l'auteur indique que « le droit à l'information de la personne concernée doit pouvoir s'opérer à tout moment par un simple clic (ou plus largement par un simple geste positif, électronique et immédiat) sur un sigle permettant l'accès à une « *Privacy Policy* » dont on peut espérer qu'elle soit d'autant plus précise et complète que le coût de la diffusion est réduit dans le cas de l'utilisation du média électronique », 52.

17 LPRPDÉ, précité, note 8, art. 4.8 Annexe 1.

II. Les étapes conduisant à l'élaboration d'une politique de confidentialité

Lorsqu'un organisme public ou un ministère, ou encore une entreprise privée décide de collecter des renseignements personnels auprès de ses usagers, de sa clientèle, certaines règles doivent être prise en considération et ce, que la collecte se fasse auprès de la personne concernée ou d'un tiers, dans le monde physique ou virtuel. Dès lors le gestionnaire se doit de répondre, entre autres, aux questions suivantes : quels sont les renseignements personnels nécessaires pour obtenir un service ou un bien, quelles sont les raisons pour lesquelles leur collecte est requise, qui y aura accès, quelle est la sécurité qui sera mise en place pour en assurer la confidentialité, comment les personnes concernées pourront exercer leurs droits et auprès de qui, quelle est la législation applicable, quels sont les moyens de recours en cas de manquement.

Cet exercice permettra au gestionnaire de déterminer ses besoins, d'envisager des solutions pour être en conformité avec les principes de protection des renseignements personnels et, de formaliser ses engagements en ce domaine. En effet, comme le rappelle le Commissariat à la protection de la vie privée du Canada :

> *L'information sur vos clients – nom, adresse, achats passés, produits préférés – est un actif commercial précieux. Contrairement à d'autres actifs, toutefois, elle ne vous appartient pas complètement. Vos clients s'intéressent à ce que vous faites des renseignements qui les concernent. Une mauvaise utilisation de l'information vous expose à des risques commerciaux. Cela pourrait nuire à votre réputation dans la collectivité, vous créer des obligations légales, entraîner des amendes et détruire la confiance essentielle aux bonnes relations avec les clients.*
> *Si vous prenez des mesures pour protéger les renseignements personnels, vous limiterez les risques et protégerez ce que vous avez investi dans un actif commercial précieux – l'information sur vos clients*.[18]

Partant, le gestionnaire doit établir une politique de confidentialité, compréhensible et accessible, indiquant ses engagements en ce qui a trait à la protection des renseignements personnels et ce, en suivant notamment les étapes décrites ci-après.

---

18 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Formation sur la protection de la vie privée (pour la petite entreprise)*, http://www.privcom.gc.ca/privacy_comm/0001_home_f.asp. Voir également, FEDERAL TRADE COMMISSION, *Protecting Personal Information – A Guide for Business*, http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html; *Privacy Policies : Say What You Mean and Mean What You Say*, Février 2008, http://www.ftc.gov/bcp/edu/pubs/articles/art09.shtm.

A. Personne responsable de la protection des renseignements personnels

Tout gestionnaire qui entend collecter et traiter des renseignements personnels, aussi bien dans le monde physique que virtuel, comme en l'espèce, doit désigner une personne qui sera responsable de la protection de ceux-ci. Dans un organisme public, cette personne pourra se voir également confier le mandat de répondre aux demandes d'accès aux documents détenus par celui-ci. Ce mandat peut aussi être attribué à une autre personne, dans ce cas il y aura un responsable de l'accès aux documents et un responsable de la protection des renseignements personnels (ci-après « responsable PRP »).

Partant, le responsable PRP doit répondre aux demandes des usagers, des clients qui souhaitent savoir quels sont les renseignements que le gestionnaire détient sur eux, ou encore qui se plaignent de l'utilisation qui en est faite. Cette personne se doit donc d'être au fait des intentions du gestionnaire en ce domaine.

Les personnes concernées (*i.e.* usagers, clients, internautes dont les renseignements personnels sont collectés) doivent pouvoir connaître l'identité et les coordonnées du responsable PRP. Seront donc, entre autres, indiqués les éléments suivants :

- ❏ nom et adresse postale de l'organisme / de l'entreprise
- ❏ nom du responsable PRP
- ❏ coordonnées de la personne responsable de la P.R.P.
- ❏ etc.

Il est à noter que ces éléments doivent figurer dans la politique de confidentialité, aussi bien dans sa version longue qu'abrégée.

À retenir

- Désigner une personne responsable de la protection des renseignements personnels
- Diffuser l'identité et les coordonnées de la personne responsable de la protection des renseignements personnels, aussi bien dans la version longue qu'abrégée de la politique de confidentialité
- Indiquer les fonctions du responsable PRP : demande d'accès et/ou traitement des plaintes

B. Renseignements personnels nécessaires à l'obtention du service ou du bien

Partant du principe que seuls les renseignements personnels pertinents / nécessaires à l'obtention d'un service ou d'un bien doivent être collectés, le gestionnaire doit déterminer quels sont les renseignements à demander aux personnes concernées. Cette détermination doit se faire en fonction de l'objet du traitement.

Ainsi, si le site Web de l'organisme public, du ministère ou de l'entreprise privée n'est qu'une vitrine visant à présenter leurs services ou leurs biens, la nécessité de collecter des renseignements personnels se fait moins ressentir que dans le cas où une interaction est envisagée avec les internautes : abonnement à un service, ouverture d'un compte client, achat-vente, réponse aux demandes, envoi d'offres promotionnelles par exemple. Dans ce cas, il convient de collecter des renseignements personnels. Mais cela ne veut pas dire que le gestionnaire peut collecter n'importe lesquels. Si la collecte du numéro de carte de crédit est utile lors d'un achat en ligne, celle-ci est moins évidente quand le site Web ne propose qu'un service de messagerie instantanée gratuit. Il est, par conséquent, important que les renseignements collectés soient en accord avec les finalités poursuivies par le gestionnaire.

Il revient donc au gestionnaire de dresser une liste des renseignements personnels qu'il entend collecter auprès des personnes concernées. Sont des renseignements personnels, par exemple :

- ❏ nom / prénom
- ❏ adresse postale
- ❏ code postal
- ❏ numéro de téléphone / télécopieur
- ❏ adresse de courriel
- ❏ date de naissance / âge
- ❏ sexe / genre
- ❏ niveau étude /
- ❏ description physique
- ❏ données de police
- ❏ numéro de carte de crédit
- ❏ numéro d'assurance maladie
- ❏ numéro d'assurance sociale
- ❏ numéro de permis de conduire
- ❏ religion
- ❏ appartenance politique / syndicale
- ❏ origines (sociales, ethniques)
- ❏ données médicales
- ❏ situation familiales
- ❏ ressources financières
- ❏ pratiques sexuelles
- ❏ etc.

En plus de collecter les renseignements personnels nécessaires / pertinents à la réalisation de l'objet, le gestionnaire peut vouloir connaître d'autres informations. Dans ce cas, il lui revient d'indiquer les données qui sont obligatoires et celles qui sont facultatives pour l'obtention du service ou du bien. Cette indication se fait généralement par le biais d'un astérisque.

À retenir
• Dresser une liste des renseignements personnels nécessaires à l'obtention du service ou du bien • Ne collecter que les seuls renseignements nécessaires • Indiquer les renseignements obligatoires et ceux qui sont facultatifs

C. Raisons de la collecte – les finalités

En même temps qu'il convient de déterminer les renseignements personnels nécessaires à la réalisation de l'objet du traitement, le gestionnaire doit établir les raisons pour lesquelles il lui faut collecter ces renseignements.

Les raisons de la collecte doivent répondre à un intérêt sérieux et légitime. Elles doivent être précises afin d'éviter toute ambiguïté quant à leur compréhension.

Parmi les raisons, il est possible de retrouver les éléments suivants :

- ❑ suivi de la commande
- ❑ contact
- ❑ statistiques
- ❑ concours / sondage
- ❑ amélioration du service
- ❑ vérification du crédit
- ❑ profil personnalisé
- ❑ informations / offres promotionnelles
- ❑ gestion du site Web
- ❑ service de plaintes
- ❑ service à la clientèle / garanties
- ❑ etc.

Dans l'éventualité où les raisons de la collecte viennent à changer, il revient au gestionnaire d'en informer les personnes concernées, soit en les contactant par courrier électronique, soit en apportant les modifications dans la politique de confidentialité accessible à tous et à tout moment.

Si la première solution est parfois utilisée, la seconde emporte davantage l'adhésion des gestionnaires d'environnements électroniques. Dans ce cas, soit les modifications sont faites sans aucune autre formalité, soit il est fait mention de la date de la dernière modification et, dans certains cas un lien existe vers les anciennes versions de la politique de confidentialité.

À retenir
• Déterminer les raisons de la collecte • Informer les personnes concernées des éventuels changements à la politique de confidentialité

D. Modalités de collecte des renseignements personnels

En principe, la collecte doit se faire par des moyens licites, honnêtes et loyaux, c'est-à-dire par des modalités perceptibles par la personne concernée. L'application de cette règle « vise à empêcher les pratiques impliquant, par exemple, l'utilisation de dispositifs secrets d'enregistrements des données »[19].

Par conséquent, si le gestionnaire entend recourir, entre autres, à des fichiers journaux (ou *log files*), à des fichiers témoins (ou *cookies*) ou à des balises de conversion / Web, il lui faut non seulement l'indiquer dans sa politique de confidentialité, mais aussi préciser les raisons d'un tel procédé.

Ainsi, lors de l'établissement de sa politique de confidentialité, le gestionnaire doit déterminer la ou les modalités de collecte des renseignements personnels. Parmi celles-ci, il est possible de retrouver les éléments suivants :

- ❑ formulaire d'inscription / d'abonnement
- ❑ formulaire de commande
- ❑ correspondance
- ❑ forum de discussion
- ❑ sondage d'opinion
- ❑ concours
- ❑ fichiers journaux
- ❑ fichiers témoins
- ❑ balises Web / images monopixels
- ❑ etc.

Quand le gestionnaire recours à des modalités de collecte dites invisibles, il lui faut également préciser dans sa politique quelles sont les informations qui sont ainsi collectées, à savoir entre autres :

- ❑ adresse IP
- ❑ système d'exploitation
- ❑ nom de domaine
- ❑ activité en ligne / pages visitées
- ❑ heure et jour de connexion
- ❑ etc.

19 ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, Paris, 23 septembre 1980, Exposé des motifs n° 52.

En précisant les modalités de collecte, visible et invisible, le gestionnaire respecte ainsi son obligation d'information, de transparence. En effet, il revient au gestionnaire d'éviter tout subterfuge lors de la collecte, et du traitement des renseignements personnels ce qui pourrait, le cas échéant, avoir une incidence sur le sentiment de confiance indispensable dans un environnement électronique.

À retenir
• Déterminer les modalités de la collecte • Informer le recours à des procédés dit invisibles et, le cas échéant, préciser les informations ainsi collectées et les raisons.

E. Personnes autorisées à accéder aux renseignements personnels

Après avoir indiqué quels sont les renseignements personnels collectés et les raisons afférentes, le gestionnaire doit préciser quelles seront les personnes qui, en dehors du responsable PRP, seront autorisées à prendre connaissance desdits renseignements. En déterminant à l'avance qu'elles seront ces personnes, le gestionnaire répond à une autre obligation : celle d'assurer la sécurité des renseignements personnels.

Il revient donc au gestionnaire de dresser une liste des personnes qui seront autorisées à accéder aux renseignements personnels. Cette liste pourra comprendre, entre autres, les personnes suivantes :

- ❑ responsable de la P.R.P
- ❑ service à la clientèle
- ❑ support technique
- ❑ webmestre
- ❑ partenaires commerciaux
- ❑ hébergeur
- ❑ fournisseurs
- ❑ annonceurs
- ❑ etc.

Dès lors, au sein de l'organisme public, du ministère ou de l'entreprise privée, il est généralement reconnu que les personnes chargées des commandes ou du service à la clientèle ont accès auxdits renseignements. Si aucune autre personne n'y a accès, il est généralement mentionné que seul le personnel autorisé - ou seul le gestionnaire - a accès aux renseignements personnels dans l'exercice de leurs fonctions.

Par ailleurs, le gestionnaire peut être amené à partager les renseignements personnels collectés avec des tiers. Cette possibilité doit être dévoilée aux personnes concernées pour qu'elles puissent, le cas échéant, s'opposer à une telle communication en exerçant leur droit d'opposition (ou *opt-in*) ou de retrait (ou *opt-out*) selon l'option choisie par l'organisme, le ministère ou l'entreprise. Partant, le gestionnaire doit

mentionner en quoi consiste ces droits et comment il est possible de les exercer. Ainsi,

- le droit d'opposition permet aux personnes concernées de refuser que leurs renseignements personnels soient utilisés à certaines fins mentionnées lors de la collecte;
- le droit de retrait permet aux personnes concernées de demander à ce que leurs renseignements personnels ne figurent plus sur une liste donnée.

Enfin, il se peut que le gestionnaire soit conduit à communiquer les renseignements personnels à des tiers en vue de répondre à ses obligations légales. La politique de confidentialité devra faire état de cette éventualité.

À retenir
• Déterminer les personnes autorisées à accéder aux renseignements personnels • Indiquer les tiers qui sont susceptibles d'avoir accès aux renseignements personnels • Indiquer comment les personnes concernées peuvent, le cas échéant, exercer leur droit d'opposition et/ou de retrait

F. Lieu de conservation des renseignements personnels

S'il est important de savoir quelles sont les personnes autorisées à accéder aux renseignements personnels collectés, indiquer le lieu de leur conservation l'est tout autant. Par conséquent, il revient au gestionnaire de préciser où seront stockés les renseignements personnels, surtout lorsqu'il est prévu que l'hébergement se fera auprès d'un tiers domicilié en dehors des frontières géographiques du gestionnaire.

Advenant cette éventualité, le gestionnaire d'où proviennent les renseignements personnels devra veiller à ce que l'entité juridique avec laquelle il fait affaire respecte, minimalement, les mêmes règles de protection. En effet, la circulation de l'information ne doit pas entraîner une réduction, voire une absence de protection.

Par conséquent, le gestionnaire doit prendre toutes les mesures nécessaires pour que les renseignements personnels bénéficient du même niveau de protection. Cette précaution est énoncée dans les lois[20], dans les recommandations des autorités de

20 *LPRPDÉ*, précité, note 8, article 4.1 Annexe 1 ; *Loi sur l'accès*, précité, note 14, article 71 ; *LPRPSP*, précité, note 14, article 17 ; *Directive 95/46/CE*, précité, note 14, article 25 ; *Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, article 68.

contrôle[21] et, est à l'origine des principes dits de la sphère de sécurité[22] (ou *Safe Harbor Principles*[23]).

À retenir
• Déterminer le lieu de conservation des renseignements personnels • Indiquer la possibilité que les renseignements personnels soient hébergés auprès d'un tiers, surtout si ce dernier situé en dehors des frontières géographiques du gestionnaire

G. Durée de conservation des renseignements personnels

En principe, les renseignements personnels ne doivent pas être conservés au-delà des raisons pour lesquelles ils ont été collectés. Ils doivent être détruit une fois l'objet du traitement réalisé. Par conséquent, le gestionnaire doit prévoir un calendrier de conservation et une procédure régissant la destruction des renseignements personnels.

À retenir
• Déterminer un calendrier de conservation • Élaborer une procédure de destruction

H. Sécurité des renseignements personnels

Le gestionnaire doit adopter des mesures visant à protéger les renseignements collectés contre, par exemple, l'utilisation, la communication, l'accès non autorisé ainsi que contre la copie, l'altération, la perte, la destruction accidentelle ou illicite. Pour éviter de telles atteintes, il revient au gestionnaire de veiller à ce que les mesures

---

21 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE AU CANADA, *Communication transfrontalière de renseignements sur les Canadiens et les Canadiennes – Répercussions de la USA Patriot Act*, Mémoire du Commissariat à la protection de la vie privée du Canada présenté au Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, 18 août 2004; *Résumé de conclusions d'enquête en vertu de la LPRPDÉ*, voir les résumés#313 et #333, http://www.privcom.gc.ca; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Transfert de données à caractère personnel vers des pays non membres de l'Union européenne*, Janvier 2007 (dernière version), http://www.cnil.fr.

22 *Décision 2000/520/CE de la Commission conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les question souvent posées y afférentes, publiés par le ministère du commerce des Etats-Unis d'Amérique*, JO L 215 du 25.8.2000, pp. 7-47.

23 Précité, note 14.

employées respectent les règles de l'art et offrent un niveau de sécurité approprié au traitement et à la nature des renseignements colligés.

Par conséquent, le gestionnaire devra préciser quelles sont les mesures mises en place pour assurer l'intégrité et la confidentialité des renseignements personnels colligés. Parmi ces mesures, il est possible de retrouver, par exemple :

- ❏ protocole SSL
- ❏ protocole SET
- ❏ gestion des accès – personne autorisée
- ❏ gestion des accès – personne concernée
- ❏ logiciel de surveillance du réseau
- ❏ sauvegarde informatique
- ❏ développement de certificat numérique
- ❏ identifiant / mot de passe
- ❏ pare-feu
- ❏ etc.

Par ailleurs, par le biais de la politique de confidentialité, le gestionnaire peut indiquer aux personnes concernées quelles sont les précautions à adopter pour assurer la confidentialité de leurs renseignements personnels, à savoir notamment : protection du mot de passe; se déconnecter après chaque utilisation, surtout sur un ordinateur public; vider la cache.

À retenir
• Déterminer les mesures de sécurité approprié au traitement et à la nature des renseignements colligés

I. Droit d'accès et de rectification des personnes concernées

Afin de permettre aux personnes concernées, d'une part, de connaître quels sont les renseignements personnels qu'un gestionnaire détient sur elles et, d'autre part, de mettre à jour ces derniers, le gestionnaire doit leur accorder un droit d'accès et de rectification.

Pour permettre l'exercice de ce droit d'accès et de rectification, il revient au gestionnaire de préciser les moyens offerts aux personnes concernées. Parmi ces moyens, il est possible de retrouver les éléments suivants :

- ❑ accès à la base de donnée / profil client
- ❑ courrier postal
- ❑ courrier électronique
- ❑ téléphone
- ❑ etc.

Si le gestionnaire permet aux personnes concernées d'accéder et de rectifier elles-mêmes leurs renseignements personnels par le biais de leur profil client, il doit veiller à ce qu'elles ne puissent pas modifier d'autres informations. Il lui revient donc de s'assurer de la gestion des accès.

À retenir
• Indiquer la procédure employée pour permettre l'exercice du droit d'accès et/ou de rectification

J. Plaintes

En cas de non-respect des engagements contenus dans la politique de confidentialité, les personnes concernées doivent pouvoir adresser une plainte soit auprès du responsable de la PRP, soit auprès de toute autre personne désignée par le gestionnaire. Il revient donc à ce dernier de préciser clairement auprès de qui une plainte peut être logée.

K. Autres

Le gestionnaire se doit d'indiquer, le cas échéant, ses engagements en matière de protection des renseignements personnels concernant des mineurs, son adhésion à un programme de certification ou encore la législation applicable.

III. Foire aux questions

Qu'est-ce qu'une politique de confidentialité ?

Une politique de confidentialité est un outil permettant à un gestionnaire d'environnement électronique d'informer les internautes de ses engagements quant au traitement des renseignements, personnels ou autres, qui seront collectés, directement ou indirectement, sur son site Web.

Que faut-il entendre par renseignements personnels ?

Un renseignement personnel est toute information permettant d'identifier une personne physique.

Qu'est-ce qu'un gestionnaire ?

Le vocable « gestionnaire » désigne tout organisme public, tout ministère ou toute entreprise privée qui entend collecter et traiter des renseignements personnels.

Qu'est-ce qu'un responsable PRP ?

Le vocable « responsable PRP » désigne la personne, nommée par le gestionnaire, qui est responsable de la protection des renseignements personnels. L'identité et les coordonnées de cette personne doivent être mentionnées dans la politique de confidentialité, aussi bien dans sa version longue qu'abrégée.

Qu'est-ce qu'une personne concernée ?

Le vocable « personne concernée » désigne toute personne physique qu'un renseignement personnel permet d'identifier.

Pourquoi élaborer une politique de confidentialité ?

En mettant en place une politique de confidentialité, un gestionnaire d'environnement électronique, en plus de répondre à ses obligations légales, fait preuve de transparence quant au traitement des renseignements, personnels ou autres, qui seront collectés sur son site. Cette transparence vise à établir un lien de confiance envers l'internaute.

Comment élaborer une politique de confidentialité ?

Dans un premier temps, un gestionnaire d'environnement électronique doit, entre autres, se poser les questions suivantes :

- des renseignements, personnels ou autres, seront-ils collectés ?
  - si oui :
    - quels sont les renseignements, personnels ou autres, qui seront collectés ?
    - comment seront collectés ces renseignements ? directement auprès de la personne concernée ? ou indirectement ? si oui, par quels procédés ?
    - pour quelle(s) finalité(s) ces renseignements sont-ils collectés ?
    - seront-ils communiqué à des tiers ? si oui, pour quelles raisons ?
    - comment seront-ils conservés ?
    - combien de temps seront-ils conservés ?
    - les personnes concernées pourront-elles accéder à leurs renseignements ? si oui, comment le pourront-elles ? qui sera en charge de traiter les demandes d'accès et, éventuellement les demandes de rectification ?
    - un mécanisme de résolution des plaintes est-il mis en place ? si oui, lequel ?
- suis-je assujetti à un instrument juridique (réglementaire ou autoréglementaire) ? si oui, lequel ?

Dans un second temps, un gestionnaire d'environnements électronique doit se demander s'il fait ou non valider sa politique de confidentialité par un organisme tiers, de type *TRUSTe* ou *BBBOnLine*.

Que faut-il entendre par droit d'accès / droit de rectification ?

Toute personne concernée a le droit de savoir quels sont les renseignements personnels qu'un gestionnaire détient sur elle. L'exercice de ce droit peut conduire à la mise à jour (droit de rectification) des renseignements ainsi conservés.

Que faut-il entendre par droit d'opposition / droit de retrait ?

Alors que le droit d'opposition permet aux personnes concernées de refuser que leurs renseignements personnels soient utilisés à certaines fins mentionnées lors de la collecte, le droit de retrait leur permet de demander à ce que leurs renseignements personnels ne figurent plus sur une liste donnée. Le premier s'exerce *a priori* alors que le second se fait *a posteriori*.

Quels sont les éléments devant être contenus dans une politique de confidentialité ?

Une politique de confidentialité doit répondre, entre autres, aux questions suivantes : quoi, pourquoi, pour qui, comment, quelle sécurité, quels sont les droits des personnes concernées. Chacune de ces questions fait référence à un ou à plusieurs des principes énoncés dans les *Lignes directrices de l'OCDE*. Ces principes, rédigés en termes généraux et repris dans de nombreux instruments juridiques (réglementaire et autoréglementaire), constituent des *minima* que toute personne souhaitant effectuer un traitement de renseignements personnels se doit de respecter.

Où doit être affichée une politique de confidentialité ?

Considérant qu'une politique de confidentialité doit être facilement accessible aux internautes, il est recommandé que celle-ci soit affichée sur la page d'accueil du site Web, préférablement sur l'ensemble des pages de ce dernier.

Qu'arrive-t-il en cas de non-respect des engagements énoncés dans une politique de confidentialité ?

Une politique de confidentialité s'entend comme étant un contrat entre le gestionnaire de l'environnement électronique et un internaute. Par conséquent, tout manquement de la part du gestionnaire quant à ses engagements entraîne sa responsabilité et, ouvre droit à réparation.

IV. Grille de vérification pour l'élaboration d'une politique modèle

Cette grille propose, sous forme de liste, les éléments devant être pris en considération par les gestionnaires d'environnements électroniques lors de l'élaboration de leurs politiques de confidentialité.

- ❑ **Responsable de la protection des renseignements personnels**
  - nomination
  - indication de son identité et de ses coordonnées
- ❑ **Collecte des renseignements personnels**
  - indication des renseignements personnels nécessaires / pertinents / obligatoires
  - indication des renseignements personnels facultatifs
  - indication des raisons de la collecte
  - indication des modalités de la collecte
- ❑ **Traitement / Utilisation des renseignements personnels**
  - indication des personnes autorisées à accéder aux renseignements personnels
  - précision du lieu de conservation des renseignements personnels
  - précision de la durée de conservation des renseignements personnels
  - indication des modalités d'exercice des droits d'opposition et/ou de retrait
- ❑ **Sécurité**
  - indication des procédés utilisés
- ❑ **Droit d'accès et de rectification**
  - indication des modalités d'exercice des droits d'accès et/ou de rectification
- ❑ **Plainte**
  - déterminer auprès de qui et quelles sont les modalités pour déposer une plainte
- ❑ **Protection des mineurs**
- ❑ **Sceau de certification**
- ❑ **Législation**