# *Chapitre 9 – La protection des informations à caractère personnel*

par Cynthia CHASSIGNEUX

## Introduction

Dans le contexte d'un environnement dématérialisé et ouvert tel qu'Internet, la collecte et l'utilisation de renseignements personnels affectent sensiblement la relation entre le commerçant et ses consommateurs. De nombreuses entreprises en ligne travaillent dès lors à construire une relation de confiance avec leurs clients. Le principal vecteur de cette approche consiste actuellement à élaborer une politique en matière de renseignements personnels. En effet, les internautes sont plus enclins à communiquer des renseignements personnels si le site Web qu'ils visitent semble assurer la confidentialité de leurs informations. Dans cette perspective, la première section de ce chapitre présente les différents aspects que le commerçant électronique doit considérer lors de l'élaboration de cette politique.

L'établissement d'un lien de confiance ne constitue pas la seule justification de l'intérêt porté à la protection des informations à caractère personnel. Le commerçant électronique doit également se soucier des normes juridiques auxquelles il risque d'être soumis et adapter en conséquence tant ses activités que sa politique. Pour cette raison, la deuxième section expose les règles légales en la matière, au niveau international, régional et national.

L'existence de règles légales ne suffit pas toujours à rassurer les internautes. En effet, les protections varient d'une juridiction à l'autre et, en conséquence, ne conviennent pas à tous les consommateurs. Compte tenu de cette réalité, les commerçants électroniques doivent recourir à des garanties complémentaires susceptibles d'établir une véritable relation de confiance. Ces solutions sont présentées dans la troisième et dernière section de ce chapitre.

## Les éléments de la politique relative aux informations à caractère personnel

Sur Internet, la protection des renseignements personnels est devenue un enjeu économique avec lequel il convient de composer. D'un côté, les commerçants veulent obtenir de plus en plus d'informations sur les personnes visitant leur site Web, à leur insu ou non, afin de maximiser leurs ventes. D'un autre côté, les consommateurs veulent tout mais en en donnant le moins.

Compte tenu de cette dynamique, certaines précisions doivent être apportées en ce qui concerne plusieurs aspects qu'un commerçant électronique doit considérer lors de l'élaboration de ses engagements envers ses consommateurs, dont principalement la collecte de renseignements personnels.

### ► La collecte de renseignements personnels

Le commerçant, que se soit dans le monde physique ou sur Internet, a besoin d'obtenir des renseignements sur son cocontractant. En effet, pour pouvoir établir un bon de commande ou une réservation, il doit demander l'identité de l'acheteur. Il doit notamment prendre connaissance des coordonnées postale et/ou électronique pour pouvoir effectuer une livraison et obtenir le numéro de carte bancaire pour paiement. Ces exemples illustrent l'importance de collecter des renseignements personnels dans le cadre d'une relation d'affaire.

Les données personnelles regroupent non seulement les noms et prénoms, l'adresse postale, les numéros de téléphone, de carte bancaire, de sécurité sociale, la date de naissance, mais aussi les adresses électroniques et IP. Toutes ces informations font partie intégrante de la notion de renseignements personnels. Dans la plupart des cas, elles identifient ou permettent d'identifier, séparément ou collectivement, une personne.

Par conséquent, pour pouvoir collecter les données personnelles, le commerçant électronique devrait demander le consentement du consommateur ou, du moins, leur indiquer que certaines informations sont collectées à leur insu, notamment à l'aide des fichiers témoins. Cette requête doit être contenue soit dans le cadre de sa politique accessible sur la page d'accueil (à défaut de l'être sur toutes les pages du site Web), soit au début du document électronique (formulaire, contrat) que les consommateurs doivent remplir. Dans ce dernier cas, il n'est pas nécessaire de réécrire l'intégralité de la politique, un résumé ou un lien vers celle-ci est suffisant. Ainsi, les personnes souhaitant commercer avec un site Web donné en connaîtront les objectifs en matière d'informations à caractère personnel.

De plus, le commerçant électronique devrait mentionner quelles sont les données qui doivent obligatoirement être collectées et celles qui ne le sont pas. Pour ce faire, il lui est possible soit de faire précéder le champ obligatoire d'un signe distinctif (astérisque, couleur), soit de générer une page mentionnant les champs omis par l'internaute lorsque ce dernier soumet le document. Ainsi, en cliquant sur un icône de type « J'accepte » ou en remplissant le document préétablis, l'internaute est supposé avoir donné son consentement. Dès lors, un nécessaire climat de confiance s'établit entre deux personnes qui souvent ne se connaissent pas.

Toutefois, ces simples mentions ne suffisent pas. Le commerçant électronique devrait permettre aux internautes de contrôler leurs informations, c'est-à-dire leur accorder un droit d'accès, de rectification et de retrait. Il devrait également informer ses consommateurs de la finalité du traitement, telle que le suivi de la commande, l'envoi de messages promotionnels, la production des statistiques et, plus spécifiquement, la diffusion et la commercialisation de leurs renseignements personnels.

### ► La diffusion et la commercialisation de renseignements personnels

Par diffusion des renseignements personnels, il convient d'entendre non seulement la mise en ligne des informations par le site Web, mais aussi l'échange, voire la commercialisation desdites données.

Quel que soit le sens retenu, il est important de rappeler que, là encore, le commerçant électronique doit obtenir le consentement de l'internaute. Cependant, les gestionnaires de sites Web peuvent être amenés à divulguer des renseignements personnels sans le consentement de la personne concernée. En effet, ils ne peuvent déroger aux obligations qui leurs sont imposées par la loi. C'est pourquoi, les responsables de sites Web devront parfois dévoiler les informations qu'ils ont en leur possession pour permettre l'identification, l'interpellation ou la poursuite en justice de tout internaute pouvant nuire à leurs intérêts ou à ceux d'autrui via leur site Web. La mention d'une telle obligation dans la politique d'un site Web marchand n'est pas impérative, mais il est tout de même préférable d'en faire allusion à titre indicatif.

Mis à part cette situation particulière, le consentement sollicité par le commerçant électronique sera bien souvent le même que celui donné lors de la collecte. Il est possible cependant que le document électronique contienne une case spécifique à cet égard. En effet, ce n'est pas parce que l'internaute autorise la détention de renseignements le concernant qu'il en permet la diffusion.

D'une part, il peut s'opposer directement, au moment de l'enregistrement, à la communication de ses données. Pour ce faire, selon le type de formulaire retenu, l'internaute devra soit activer l'option, soit la désactiver. Il s'agit de la technique du *opt-in*. D'autre part, l'internaute peut agir ultérieurement en demandant, par courrier postal ou électronique, que ses renseignements ne soient plus divulgués à des tiers. On parle alors de la technique du *opt-out*.

Ces techniques du *opt-in* et du *opt-out* sont le plus souvent utilisées lorsque le commerçant électronique prévoit faire du marketing direct, en informant, par exemple, sa clientèle des offres promotionnelles et des mises à jour de son site Web. Ces offres peuvent mettre en avant les biens et/ou services du site Web marchand ou encore ceux de ses partenaires commerciaux. En effet, ils peuvent confier des messages publicitaires au gestionnaire du site en lui précisant le type de public visé, à lui par la suite de diffuser le contenu de la réclame aux personnes correspondant aux critères prédéfinis. Dans ce cas, le commerçant est le seul à accéder aux données personnelles qu'il détient. Il se peut cependant que le commerçant transmette certaines informations à ses partenaires. Pour ce faire, il doit obtenir le consentement de la personne intéressée avant le transfert desdites données, notamment lorsque l'opération a pour but d'interconnecter plusieurs fichiers contenant des renseignements personnels.

### ► L'interconnexion de fichiers

Par interconnexion, il convient d'entendre le fait pour une même entreprise, voire plusieurs, de regrouper différents types d'informations concernant une même personne ou une catégorie de personne. Ainsi, une entreprise peut connaître à partir d'un nom donné, non seulement l'état de santé de la personne, son cursus universitaire, ses préférences en matière de divertissement, mais aussi ses infractions au code de la route, voire son dossier bancaire ou judiciaire.

Cette technique utilisée par les banques, les assureurs, les employeurs est loin d'être nouvelle. Elle est simplement facilitée et amplifiée depuis l'informatisation des fichiers. Dès lors, certaines critiques s'élèvent. En effet, les fusions d'entreprises, la découverte de fichiers nationaux liant plusieurs bases de données entre elles font peser une menace sur la vie privée des personnes.

Cette crainte est encore plus grande avec le développement des inforoutes et du commerce électronique. C'est pourquoi, en principe, l'interconnexion de fichiers est soumise au respect de la loi afin d'éviter que de tels agissements ne débouchent sur des discriminations, des congédiements, des atteintes à la vie privée. Or, comment contrôler qu'une entreprise située dans un pays A ne compile pas les données qu'elle détient avec la société mère, une filiale ou un partenaire situé dans un pays B ? Comment s'assurer qu'un site Web ne connaît pas déjà le profil de consommation d'un internaute lors de sa première visite sur son site ?

Par conséquent, si un commerçant électronique entend mettre en relation ses bases de données avec celles constituées par d'autres sites Web, il doit préalablement en informer sa clientèle en vue d'obtenir son consentement.

Le consentement constitue, comme nous avons pu le constater, un élément essentiel dans le rapport qui s'établit entre le commerçant électronique et le consommateur-internaute. Néanmoins, cette relation peut être remise en cause lorsque l'entreprise utilise, à son insu, de nouveaux procédés de collecte, tels que l'emploi de fichiers journaux et de fichiers témoins.

### ► Les fichiers journaux et les fichiers témoins

Les fichiers journaux (*log file*) emmagasinent des informations sur l'adresse IP des visiteurs, les pages Web qu'ils ont fréquentés ainsi que le type d'ordinateur qu'ils utilisent. En principe, il y a donc un risque de porter atteinte à la vie privée des internautes. En effet, les commerçants électroniques utilisent généralement les fichiers journaux pour dresser des statistiques et plus particulièrement pour déterminer les habitudes personnelles des consommateurs. Cette dernière possibilité est toutefois limitée par l'attribution rotative des adresses IP par la plupart des FAI à leurs abonnés. Néanmoins, l'utilisation de fichiers journaux demeure problématique au regard de la protection des renseignements personnels dans la mesure où le FAI conserve les informations relatives à l'attribution des adresses IP. Le commerçant électronique devrait donc mentionner, notamment dans sa politique relative aux informations à caractère personnel, l'utilisation qu'il entend faire avec les données des fichiers journaux.

En raison du manque de précision des données contenues dans les fichiers journaux, les entreprises en ligne ont recours aux fichiers témoins (*cookies*). Ces derniers permettent d'attribuer un numéro unique à chaque visiteur et ainsi suivre les consommateurs peu importe leur adresse IP. Il faut cependant préciser qu'à l'origine ce procédé a été développé pour faciliter la navigation. Par la suite, les fichiers témoins ont été utilisés pour (re)tracer, voire créer le profil des usagers qui se connectent à un site Web.

Contrairement à l'idée répandue, l'utilisation de ce procédé n'est pas spécialement litigieuse. Il en va différemment lorsque le commerçant électronique associe le numéro unique du fichier témoin à des renseignements personnels autrement collectés, c'est-à-

dire lors d'une inscription ou d'un achat en ligne. En permettant l'identification des internautes, cette combinaison d'informations devient illicite dans la plupart des États qui ont adopté des dispositions visant à protéger les informations à caractère personnel.

En conséquence, les sites Web marchands devraient prévenir les internautes de l'existence et de l'utilisation des fichiers témoins. Cet avertissement sera le plus souvent contenu dans la politique de confidentialité du site Web. Le commerçant doit donc indiquer non seulement la nature du fichier témoin, mais aussi les raisons pour lesquelles il utilise une telle technique, à savoir à des fins d'identification, de statistiques ou autres.

Une fois le visiteur identifié, seul le commerçant électronique peut lire les informations inscrites par les fichiers témoins placés dans l'ordinateur de ses clients. Toutefois, plusieurs entreprises permettent à des régies publicitaires d'implanter des fichiers témoins chez leurs visiteurs et ainsi de prendre connaissance d'informations relatives à leur navigation sur plusieurs sites.

### ► Les régies publicitaires en ligne

Les régies publicitaires permettent à des entreprises de déléguer la gestion de leur portefeuille publicitaire. Or, dans le contexte des inforoutes, elles ont développé une stratégie d'ensemble qui consiste à recourir aux fichiers témoins et à dresser des profils de cyberconsommateurs. Plus particulièrement, elles ont mis en place des réseaux de partenaires leur permettant d'opérer sur un large panel, notamment par l'entremise de bandeaux publicitaires placés en ligne. En effet, ces derniers dirigent souvent le consommateur vers un site membre du réseau.

À titre d'illustration, la régie publicitaire *DoubleClick* propose à ses membres un important réseau de sites Web affiliés utilisant entre autre des bandeaux publicitaires. Ainsi, en naviguant sur les sites ayant adhérés à *DoubleClick*, le profil de consommation de l'internaute se dessine de clic en clic. Dès lors, l'internaute ne sera plus simplement identifié comme étant « Monsieur X, utilisant tel système d'exploitation, s'étant connecté au site Web il y a de cela trois jours », mais comme étant « Monsieur X, allant régulièrement acheter des livres, aimant les sites musicaux et jouant régulièrement aux casinos virtuels ». Pour résultat, des publicités ciblées lui seront proposées afin d'attirer son attention.

Loin de faire l'unanimité, cette stratégie a fait l'objet de nombreuses critiques au courant de l'année 1999 particulièrement lors du rachat de la société *AbacusDirect* par *DoubleClick*. Il s'agit d'une entreprise spécialisée en marketing direct et possédant une importante base de données nominatives constituée à partir des achats effectués par correspondance postale – et non en ligne.

À la suite de cette fusion, les associations de défense et les particuliers ont craint un croisement de leurs informations. De nombreux sites Web ont donc décidé de réduire, voire de mettre fin à leur adhésion à *DoubleClick*. En conséquence, la régie a modifié sa politique. Désormais, tout internaute qui ne souhaite plus figurer dans les listes de la régie publicitaire devra en faire la demande via le site Web de *DoubleClick*. Par conséquent, si l'internaute n'utilise pas la technique du *opt-out*, il continuera à être suivi par défaut …

Pour éviter toute controverse, le commerçant électronique devrait faire apparaître dans sa politique une section relative aux régies publicitaires, en indiquant entre autres :

- l'existence de fichiers témoins sur son site Web, que ceux-ci soit mis en place pour son propre compte ou par une agence de publicité ;
- l'adhésion ou non avec une régie publicitaire. Il est important de préciser le nom, voire de faire un lien vers le site de cette régie ou agence de publicité. Ainsi, les internautes pourront se renseigner sur la politique de cette dernière ;
- la finalité de ce partenariat ;
- les conséquences pour un internaute d'accéder à un autre site Web par le biais d'une bannière publicitaire ;
- etc.

Les procédés des régies publicitaires concernent particulièrement la protection des renseignements personnels. Toutefois, les aspects de la vie privée sur Internet ne se limitent pas à ces seules données. En effet, d'autres d'informations risquent d'être collectées et divulguées par les commerçants électroniques.

### ► Les données sensibles

Les données sensibles sont des informations qui ont trait entre autres à l'origine raciale, aux opinions politiques, religieuses, syndicales, à la vie sexuelle et à l'état de santé. Le traitement de ces données fait l'objet d'une attention particulière de la part des États, certains allant même jusqu'à en réglementer l'utilisation.

En ce qui concerne, par exemple, les données médicales, celles-ci comprennent toutes informations relatives à la santé d'une personne, à savoir ses antécédents familiaux, ses pathologies, ses médications, etc. Ces données comprennent également toutes informations ayant trait à l'identification de la personne auprès des organismes de santé, de sécurité et d'aide sociale, mais aussi toutes les notes personnelles du médecin soignant. En général, ces informations sont consignées dans un ou plusieurs dossiers médicaux tenus par le ou les praticiens consultés par le patient.

En principe, le médecin doit obtenir le consentement de son patient avant d'ouvrir un dossier à son nom. Or, il est possible de dire que l'accord de la personne est tacite, une telle pratique faisant partie des règles du métier. Cependant, on peut se demander si le principe ne doit pas être renforcé compte tenu de l'informatisation grandissante des dossiers médicaux ? Cette question prend une dimension toute particulière depuis quelques années. En effet, depuis l'informatisation des professionnels de la santé, des réseaux spécialisés ainsi que des sites Web « médicalisés » se développent.

Ces sites Web permettent notamment d'obtenir une consultation en ligne et la livraison à domicile de médicaments moyennant quelques renseignements. En conséquence, il importe que le propriétaire du site Web mette en œuvre tous les moyens nécessaires pour assurer la sécurité du traitement et tenir compte de ce qui a été précédemment mentionné en ce qui a trait aux renseignements personnels.

La précaution nécessaire dans le traitement des données sensibles doit également se retrouver lorsqu'un site Web marchand entend diriger son activité vers un public mineur.

### ► Les enfants

Au fil des sections précédentes, nous avons passé en revue certaines questions relatives à la protection des renseignements personnels qu'il convient de considérer lorsqu'un commerçant envisage de développer un site Web marchand. Cependant, le tableau ne pourrait pas être complet si nous ne prenions pas en compte les enfants.

Le réseau étant accessible à tout le monde, personne ne peut savoir si vous êtes un adulte, un mineur … ou même un chien installé devant votre ordinateur. Pendant longtemps cette image a fait le tour du réseau. Or, on constate de plus en plus qu'il est possible pour un gestionnaire de site Web de savoir que la personne qui est à l'autre bout de la ligne est un enfant. Il est donc possible pour un site Web d'orienter certaines, voire la totalité de ses activités vers ces nouveaux internautes, les enfants constituant une importante part de marché que ce soit en termes d'audience, de fréquentation ou encore de revenus.

Par conséquent, la protection accordée aux internautes-adultes doit être étendue aux internautes-enfants. En effet, tout comme les adultes, ils doivent pouvoir naviguer en toute connaissance de cause, et donc donner leur accord à l'utilisation de leurs renseignements personnels. Face à cela, on peut se demander qu'elle est la valeur d'un consentement émis par un enfant ? Ce dernier est-il en mesure de réaliser toutes les implications reliées à l'implantation d'un fichier témoin dans le disque dur de l'ordinateur de ses parents ?

Dès lors, si les enfants sont la cible d'un site Web marchand, le commerçant doit obtenir le consentement d'un adulte avant que l'enfant n'accède à ses biens et services. Ce dernier ne peut pas accepter pour lui-même puisque sa faculté est juridiquement réduite en raison de son âge.

La mise en place de telle politique permet à l'internaute de naviguer sur le site Web avec le sentiment d'en connaître un peu plus sur les intentions des commerçants électroniques. Pour renforcer le sentiment de confiance qui s'instaure, des voix s'élèvent de part et d'autre pour encadrer la protection des renseignements personnels soit en ayant recours à des outils réglementaires, soit en laissant le réseau se réguler par lui-même.

## Les protections légales

La protection accordée aux renseignements personnels varie d'un État à l'autre. À ce titre, il est possible de schématiser et de constater que dans les pays de *common law*, la protection des renseignements personnels se fait de façon sectorielle. L'encadrement est plus important dans le secteur public que dans le secteur privé, celui-ci étant soumis à la loi des parties, voire à leur propre réglementation (autoréglementation). Cependant, depuis quelques années, on assiste à un changement d'orientation des pays de *common law*. Ces derniers envisagent, comme dans les pays de droit civil, une protection des secteurs public et privé. En effet, les pays de droit civil protègent l'individu tant dans ses rapports avec l'État, qu'avec les entreprises privées et les particuliers. Cette protection peut concerner tant le droit civil que le droit pénal.

Dès lors, même si l'étude des règles mises en place par les institutions nationales, régionales, provinciales ou internationales peut surprendre dans un espace qui ne connaît pas de frontières, il nous faut les prendre en considération. En effet, il convient de

signaler que l'application de ces normes peut être obligatoire notamment selon le lieu – physique – d'enregistrement du site Web marchand (peu importe que le nom de domaine de tête générique soit un .com ou un .fr par exemple). C'est pourquoi on assiste de plus en plus à une « fuite » des entreprises vers des zones géographiques n'accordant peu ou prou de protection aux renseignements personnels.

Ne pouvant prendre en considération l'ensemble des textes, nous arrêterons notre choix sur certains d'entre eux pouvant s'appliquer à la protection en ligne des renseignements à caractère personnel.

**► Les Lignes directrices de l'Organisation de Coopération et de Développement Économique (OCDE)**

L'OCDE travaille sur une base égalitaire pour encourager le développement du commerce mondial entre les vingt-neuf pays membres à savoir :

- Australie
- Canada
- Corée
- États-Unis
- Hongrie
- Islande
- Japon
- Mexique
- Norvège
- Nouvelle-Zélande
- Pologne
- République Tchèque
- Suisse
- Turquie
- Les 15 États membres de l'Union européenne

Les textes adoptés par les membres de l'OCDE sont le reflet d'un dialogue pouvant donner lieu à des discussions avec des pays non membres. À ce titre l'OCDE a de nombreux contacts avec les pays d'Asie, d'Amérique Latine, de l'ancien bloc soviétique et d'Afrique. Ces échanges permettent un rapprochement et la communication de différents points de vues. Pour avoir une vision d'ensemble, l'OCDE est en effet tenu de considérer des influences du monde entier. Dans le même ordre d'idée, l'OCDE doit suivre les évolutions technologiques susceptibles d'avoir des répercussions sur le commerce et sur la société en général.

C'est dans ce cadre que l'OCDE a mis en place différents textes visant à protéger la vie privée des citoyens, et donc des internautes. Le plus important en la matière a été adopté le 23 septembre 1980 sous le titre de *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel* (Lignes directrices de l'OCDE). Ce texte, visant à harmoniser les législations nationales des pays signataires, concentre son attention sur la protection des données à caractère personnel qui circulent au-delà des frontières. Pour atteindre cet objectif, les Lignes directrices de l'OCDE préconisent un ensemble de principes technologiquement neutres et couvrant aussi bien le secteur public que privé.

Ainsi, 20 ans après leur mise en vigueur, la validité des Lignes directrices de l'OCDE n'est pas remise en cause et peuvent donc s'appliquer sur le réseau des réseaux. En effet, elles énoncent des principes fondamentaux en matière de traitement des données à caractère personnel qu'un site Web peut collecter.

Par conséquent, sans faire expressément référence aux Lignes directrices de l'OCDE, les politiques relatives aux renseignements personnels adoptées par les sites Web marchands reprennent majoritairement les principes suivants :

- *limitation en matière de collecte* (paragraphe 7), c'est-à-dire que les méthodes de collecte de l'information doivent être loyales et licites. Par voie de conséquence, et comme nous l'avons déjà mentionné, cette collecte ne doit pouvoir se faire qu'après en avoir informé la personne concernée ou encore après avoir obtenu son consentement ;
- *qualité des données* (paragraphe 8), c'est-à-dire que les données recueillies ne doivent pas dépasser les finalités du traitement. Ainsi, un site Web marchand offrant des services gratuits, comme par exemple un service de messagerie électronique, ne doit pas demander le numéro de sécurité sociale ou de carte bancaire. En effet, ces informations ne sont pas nécessaires à la création du nom d'usager et du mot de passe de l'internaute. De plus, le commerçant électronique doit s'assurer que les renseignements qu'il possède sont exacts, complets et mis à jour, pour éviter toute confusion ;
- *spécification des finalités* (paragraphe 9), c'est-à-dire que le site Web marchand doit indiquer les raisons de la collecte. Le commerçant électronique va-t-il emmagasiner ces informations à des fins de statistique, de marketing, d'identification ? Il est important que cette précision soit communiquée à l'internaute avant qu'il ne saisisse ses données. De cette façon, l'internaute pourra consentir à la collecte en toute connaissance de cause ;
- *limitation de l'utilisation* (paragraphe 10), c'est-à-dire que les données recueillies ne doivent pas être divulguées, utilisées à des fins autres que celles spécifiées au moment de la collecte à moins que la personne concernée n'y consente ou que cette divulgation est nécessaire au commerçant électronique pour répondre à ses obligations légales.
    - La limitation de l'utilisation pourra se faire par la faculté reconnue à l'internaute de s'opposer, non seulement par les instruments légaux, mais aussi par la technique du *opt-in* ou du *opt-out*, à la communication de ses renseignements personnels à toute autre personne que le commerçant électronique ;
- *garanties de sécurité* (paragraphe 11), c'est-à-dire protéger les données contre leur perte, leur accès, destruction, utilisation ou divulgation non autorisés ;
- *transparence* (paragraphe 12), c'est-à-dire que la politique de protection des données personnelles doit être claire. Elle doit au moins être accessible sur la page principale, si ce n'est sur toutes les pages du site Web;
- *participation individuelle* (paragraphe 13), c'est-à-dire que le commerçant électronique doit permettre à tout internaute qui le souhaite d'obtenir copie des informations qu'il détient sur lui. Ainsi il pourra soit les corriger, les compléter, voire demandez leur destruction.
    - Pour permettre à l'internaute d'exercer son droit, le commerçant électronique doit soit créer un lien vers le courrier électronique de la personne étant en charge de répondre à de telles demandes, soit prévoir un formulaire à cet effet sur le site Web, soit communiquer l'adresse postale à laquelle il est possible pour l'internaute d'obtenir de telles informations.
    - L'indication de l'adresse postale semble être obligatoire selon certaines législations, non seulement par soucis de transparence, mais aussi pour permettre à l'internaute de communiquer avec les responsables du site Web marchand autrement que par voie électronique ;
- *responsabilité* (paragraphe 14), c'est-à-dire qu'en cas de non respect des principes ci-dessus le commerçant électronique pourra faire l'objet de poursuite pour atteinte à la vie privée. C'est pourquoi le commerçant électronique

indiquera, dans sa politique ou dans les conditions d'utilisation du site Web, non seulement des clauses limitatives de responsabilité, mais aussi le ressort de la juridiction compétente en cas de conflits ou encore qu'il entend soumettre tous les différends susceptibles de naître à la médiation ou à l'arbitrage traditionnel ou en ligne.

Les Lignes directrices de l'OCDE régissent, comme nous venons de le voir, la collecte, l'utilisation et la gestion des renseignements personnels. Elles préconisent également la mise en place de moyens sécuritaires, tels que la cryptographie, pour permettre la transmission en ligne de ces informations à l'extérieur des frontières d'un territoire. À cet égard, il convient de mentionner que l'OCDE a adopté le 26 novembre 1992 des *Lignes directrices relatives à la sécurité des systèmes d'information.*

Au lendemain de l'adoption des Lignes directrices de l'OCDE, le Conseil de l'Europe et l'Union européenne ont élaboré différents instruments juridiques qui, contrairement aux Lignes directrices de l'OCDE qui ne sont que de simples recommandations, sont contraignants pour les pays européens.

### ► Les instruments juridiques européens

Avant de d'analyser les instruments juridiques européens, il nous semble important de faire mention de quelques précisions au sujet non seulement du Conseil de l'Europe, mais aussi de l'Union européenne. Il s'agit en effet de deux organisations différentes qu'il est courant de confondre.

Le Conseil de l'Europe est une organisation intergouvernementale qui a pour objectif de défendre les droits de l'homme, de favoriser le développement de l'identité culturelle de l'Europe. Le Conseil de l'Europe, outre les invités spéciaux et les observateurs que sont par exemple le Canada, Israël, le Japon, le Mexique et les États-Unis, rassemble quarante et un pays membres, à savoir :

- Albanie
- Andorre
- Bulgarie
- Croatie
- Chypre
- République Tchèque
- Estonie
- Géorgie
- Hongrie
- Islande
- Lettonie
- Liechtenstein
- Lituanie
- Malte
- Moldavie
- Norvège
- Pologne
- Roumanie
- Fédération de Russie
- Saint Martin
- Slovaquie
- Slovénie
- Suisse
- L'ex république yougoslave de Macédoine
- Turquie
- Ukraine
- Les 15 États membres de l'Union européenne

La mission du Conseil de l'Europe consiste à débattre de questions de société. À ce titre, il a adopté, le 28 janvier 1981, la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* (Convention 108). Ce texte a été ratifié par la Hongrie, l'Islande, la Norvège, la Slovénie, la Suisse et l'Union européenne.

La Convention 108 a pour but, aux termes de son article 3-1, « de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa

résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant », que ce soit dans le secteur public ou privé.

Pour arriver à cet objectif, la Convention 108 a établi des « Principes de base pour la protection des données ». Ces principes, tout comme ceux des Lignes directrices de l'OCDE, reflètent les domaines qu'il convient de respecter dès que l'on veut collecter des renseignements personnels. Il est donc possible, là encore, que la politique d'un site Web marchand en matière de renseignements personnels s'inspire de ces derniers, comme par exemple :

- *la qualité des données* (article 5). En l'espèce cela signifie que la collecte doit être licite et loyale, pour des finalités spécifiées préalablement à la personne concernée, et l'utilisation de ces données ne doit pas contrevenir avec ce qui a été prévu à l'origine, etc. ;
- *la sécurité des données* (article 7), c'est-à-dire que le gestionnaire du site Web doit être en mesure de prévenir tout risque de destruction, de perte, d'accès par des personnes non autorisées ;
- *les garanties complémentaires pour la personne concernée* (article 8), c'est-à-dire que l'internaute doit avoir la possibilité d'accéder, de modifier, d'effacer sur simple demande les données le concernant. En cas de refus, celui-ci peut engager des poursuites contre le gestionnaire du site Web.

Il est également précisé que certaines données ne peuvent pas faire l'objet d'un traitement, sauf si ce dernier est prévu en droit interne. Par conséquent, sont considérées comme des données sensibles, aux termes de l'article 6, celles :

> « […] révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle […]. Il en est de même des données à caractère personnel concernant des condamnations pénales ».

Cependant, même si un site Web marchand est tenu de garantir la sécurité et la confidentialité des données qu'il a recueillies avec le consentement de la personne concernée, il peut arriver que le commerçant électronique soit obligé de divulguer ces informations pour répondre à ses obligations légales.

La Convention 108, tout comme les Lignes directrices de l'OCDE, peut être considérée comme un instrument international visant à protéger la collecte, l'utilisation et la diffusion des données à l'intérieur des pays membres du Conseil de l'Europe, mais également à l'extérieur de cette zone géographique. En effet, la Convention 108 est ouverte à l'adhésion de pays non membres, ce qui n'est pas le cas des textes mis en place par l'Union européenne.

L'Union européenne a pour mission de promouvoir un équilibre économique et sociable durable entre les quinze États membres, à savoir :

- Allemagne
- Autriche
- Belgique
- Danemark
- Espagne
- Finlande
- France
- Grèce
- Irlande
- Italie
- Luxembourg
- Pays-Bas
- Portugal
- Royaume-Uni
- Suède

Pour ce faire, elle dispose de cinq institutions (Parlement européen, Conseil de l'Union européenne, Commission européenne, Cour de justice, Cour des comptes) qui, soutenues par plusieurs organes, adoptent des règlements, des directives, des décisions, des avis, des recommandations et des actes non prévus.

C'est par le recours à une directive que l'Union européenne a entendu protéger les renseignements personnels entre les États membres. Les directives sont des actes qui, d'une part, visent à harmoniser les législations et les réglementations nationales, et d'autre part, imposent une obligation de résultat aux États membres. Par conséquent, les États doivent tout mettre en œuvre pour atteindre les objectifs décrits.

La *Directive 95/46/CE* du Parlement européen et du Conseil *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* (Directive 95/46/CE) a été adopté le 24 octobre 1995. Cette directive vise à concilier la protection des données à caractère personnel avec la libre circulation de celles-ci non seulement en Europe, mais aussi en dehors des frontières, c'est-à-dire en direction de pays tiers. Cette libre circulation ne pourra se faire que si ces derniers offrent « un niveau de protection adéquat ». Nous reviendrons plus tard sur cette notion qui peut avoir des répercussions sur le transfert des données entre sites Web.

Mais avant, il convient de préciser qu'aux termes de la Directive 95/46/CE, les données doivent être adéquates aux finalités poursuivies, ne pas concerner les origines raciales, les opinions politiques, religieuses ou philosophique, l'appartenance syndicale, ainsi que les informations relatives à la vie sexuelle sauf si la personne concernée y a consenti.

De plus, la personne faisant l'objet de cette collecte doit être informée de l'identité des personnes qui seront en possession desdites données sur lesquelles il conserve un droit d'accès et de rectification, ainsi que le droit de s'opposer, sans motif, aux traitements ayant une finalité commerciale.

La Directive 95/46/CE reprend donc les principes de base énoncés aussi bien dans les Lignes directrices de l'OCDE que dans la Convention 108. Et tout comme la Convention 108, la Directive 95/46/CE est contraignante et doit faire l'objet d'une transposition dans le droit interne de chacun des pays membres de l'Union européenne, ce qui n'était pas encore le cas de tous deux ans après son entrée en vigueur.

Outre cette situation, le point qui soulève encore à l'heure actuelle des interrogations est celui du « niveau de protection adéquat ». En effet, la Directive 95/46/CE énonce en son article 25 que « le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat ».

Ainsi, théoriquement, depuis l'entrée en vigueur de la Directive 95/46/CE, soit le 25 octobre 1999, plus aucune donnée à caractère personnel n'est susceptible d'être transmise vers les pays tiers n'offrant pas un niveau de protection adéquat. Cette disposition touche les pays non membres de l'Union européenne, dont notamment les États-Unis. En est-il de même pour les pays européens qui n'ont pas encore transposé la Directive 95/46/CE en droit interne ? Cette situation ne semble pas porter à conséquence, lesdits États membres disposant d'une législation en la matière visant aussi bien le secteur public que privé. La protection de la vie privée et des données personnelles est donc garantie.

En conséquence, si un site Web est localisé dans l'un des quinze pays d'Europe, il est possible, lorsque le consommateur y consent, de transférer des données à travers les frontières de l'Union européenne. Par contre, il en sera autrement si le site Web veut communiquer des informations vers un site Web situé aux États-Unis par exemple. En effet, la protection est généralement assurée dans le secteur public par des textes constitutionnels, fédéraux et gouvernementaux, alors que dans le secteur privé, seules quelques domaines d'activité sont réglementés, tels que les banques ou les agences de crédits.

La protection reconnue dans le secteur privé est à la source des débats qui se sont instaurées entre l'Union européenne et le ministère du commerce américain. Toutefois, un accord est intervenu entre les parties après plusieurs mois de négociations : « *Safe Harbor* » ou « principes internationaux de la sphère de sécurité relatifs à la protection de la vie privée ». Cet accord repose sur l'idée que le ministère du commerce américain dressera une liste des entreprises qui adhéreront et s'engageront publiquement à respecter un ensemble de règles protégeant les données personnelles. Ainsi, les entreprises devront adresser une lettre mentionnant les coordonnées, les activités et la politique adoptée en matière de protection des renseignements personnels. Par la suite, le ministère pourra procéder à toutes vérifications et, en cas de fausse déclaration ou de non respect, l'organisme fera non seulement l'objet de sanctions légales, mais aussi sera retiré de la liste des entreprises assurant une protection adéquate aux données personnelles.

En somme, la Directive 95/46/CE ainsi que les Lignes directrices de l'OCDE et la Convention 108 sont de nature à protéger les données personnelles qu'un site Web recueille lors de la visite d'un internaute ou encore lorsque ce dernier remplit un document électronique pour pouvoir accéder aux biens et services proposés par le commerçant électronique. Ces textes ne sont cependant pas les seuls susceptibles de garantir la vie privée des internautes. En effet, le commerçant électronique doit également considérer la législation nationale du lieu d'enregistrement de son site Web ainsi que celle pouvant lui être applicable en raison de ses activités à l'étranger.

### ► Les législations nationales

Les législations nationales, c'est-à-dire les lois, règlements et autres décrets d'application ont forces exécutoires dès leur entrée en vigueur ou rétroactivement dans certains cas. Cela signifie que toute personne physique, toute entreprise, voire tout commerçant électronique qui entend soit domicilier son site Web sur un territoire donné soit y exercer une activité commerciale doit en respecter les règles de droit.

Sur Internet, cette obligation peut être difficile à mettre en application en raison du caractère transfrontalier de ce réseau. Si, par exemple, un commerçant électronique établit

son activité aux États-Unis mais entretient des relations avec la France, il sera soumis à deux régimes distincts de réglementation nationale. En effet, à la différence des États-Unis où règne l'autoréglementation des entreprises ayant une activité privée, plusieurs pays, dont notamment la France et le Canada, se sont dotés de règles nationales trouvant à s'appliquer à Internet.

En France, la *Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (Loi Informatique et Libertés) s'applique dès que les informations nominatives collectées, enregistrées ou conservées par une entité publique et/ou privée ont un point de contact avec le territoire français.

Cette loi emploi, dans son article 1er, la notion de « vie privée » sans en donner de définition. Elle associe à cette expression celle d'« informations nominatives ».

> « Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale. » (art. 4)

Dès lors, pour pouvoir assurer la protection des informations nominatives, leur collecte doit se faire de façon licite (art. 25). Pour ce faire, le commerçant électronique doit informer l'internaute de ses intentions, il doit lui donner un droit d'opposition (art. 26) ainsi qu'un droit d'accès et de rectification (art. 34 et suivants). De plus, il a l'obligation, avant de collecter de telles informations, de déclarer (secteur privé) (art. 16) ou de soumettre pour avis (secteur public) (art. 15) son fichier à la Commission Nationale de l'Informatique et des Libertés (CNIL) et de prendre toutes les mesures nécessaires pour assurer la sécurité de sa base de données (art. 29).

En ce qui concerne le Canada, et plus particulièrement le Québec, ce sont les *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et *Loi sur la protection des renseignements personnels dans le secteur privé* qui doivent être prises en considération par le commerçant électronique selon le secteur d'activité de son site Web. Ces deux lois viennent compléter la *Charte des droits et des libertés de la personne* et le *Code civil du Québec*. La première de ces lois ne retiendra pas longtemps notre attention. Nous préférons effectivement nous concentrer sur la seconde ayant trait au secteur privé, et faisant figure de pionnière au Canada et en Amérique du Nord. Ainsi, aux termes de l'article 1, cette loi :

> «[…] a pour objet d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du Code civil du Québec en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil du Québec. »

La loi, adoptée en 1994, s'applique quel que soit le support utilisé. Cela signifie qu'elle vise tous les renseignements personnels qui pourraient être recueillis, utilisés ou communiqués par des moyens électroniques, soit entre un commerçant et un

consommateur, soit entre deux particuliers. En protégeant les renseignements circulant sur Internet, elle couvre les mêmes objectifs que la nouvelle loi fédérale.

En effet, depuis la fin de l'année 1999, le Canada, qui jusqu'à présent ne protégeait que les renseignements personnels collectés par les gouvernements, s'est doté d'une législation visant le secteur privé, la *Loi sur la protection des renseignements personnels et les documents électroniques*.

La protection reconnue est fondée sur le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation. Ainsi, le commerçant électronique a l'obligation, selon la nouvelle loi, de respecter les principes suivants :

- *la responsabilité* (article 4.1 de l'annexe) : le commerçant électronique doit tout mettre en œuvre pour protéger les renseignements qu'il détient;
- *la détermination des fins de la collecte des renseignements* (article 4.2 de l'annexe) : le commerçant électronique doit avant ou au moment de la collecte préciser les raisons de celle-ci, afin de se conformer au principe de transparence, d'accès aux renseignements personnels, de limitation en matière de collecte. De plus, il doit obtenir le consentement de la personne intéressée avant de procéder au traitement de l'information ;
- *le consentement* (article 4.3 de l'annexe) : cela signifie que le consentement de la personne intéressée est nécessaire pour pouvoir procéder au traitement. Il peut être retiré à tout moment pour des motifs raisonnables ;
- *la limitations de la collecte* (article 4.4 de l'annexe) : le commerçant électronique ne peut recueillir que les informations nécessaires au traitement et à ce seul traitement. La collecte doit être honnête et licite ;
- *la limitation de l'utilisation, de la communication et de la conservation* (article 4.5 de l'annexe) : le commerçant électronique ne peut pas utiliser les renseignements recueillis à d'autres fins que celles prévues initialement, sauf consentement de l'intéressé. Il doit de plus conserver les renseignements pour les seuls besoins de ce traitement ;
- *l'exactitude* (article 4.6 de l'annexe) : les renseignements doivent être complets, exacts et tenus à jour ;
- *les mesures de sécurité* (article 4.7 de l'annexe) : le commerçant électronique doit tout mettre en œuvre pour sécuriser les renseignements qu'il détient (perte, vol, consultation, communication, utilisation non autorisées) en utilisant aussi bien des moyens matériels, administratifs que techniques ;
- *la transparence* (article 4.8 de l'annexe) : le commerçant électronique doit établir des politiques de gestions des renseignements personnels compréhensibles ;
- *l'accès aux renseignements personnels* (article 4.9 de l'annexe) ;
- *la possibilité de porter plainte à l'égard du non respect de ces principes* (article 4.10 de l'annexe).

On peut donc dire que la loi canadienne reprend non seulement les principes mis en place par les Lignes directrices de l'OCDE, mais entend aussi favoriser le rapprochement des législations fédérales et provinciales en matière de protection des données personnelles. Pour ce faire, et pour tenir compte des législations provinciales en la matière, l'article 30(1) de la loi prévoit une période de transition de trois ans pendant laquelle elle ne s'appliquera pas :

> « […] à une organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique dans une province dont la législature a le pouvoir de régir la collecte, l'utilisation ou la communication de tels renseignements, sauf si elle le fait dans le cadre d'une entreprise fédérale ou qu'elle communique ces renseignements pour contrepartie à l'extérieur de cette province. »

En vertu de cette loi, le Canada dispose ainsi, tout comme le Québec, d'un niveau de protection adéquat correspondant probablement aux attentes de la Directive 95/46/CE. Par conséquent, un site Web situé en Europe pourrait, si un consentement a été donné à cet effet, transférer des données vers des partenaires situés au Canada, et inversement.

Internet, comme nous pouvons le constater, n'est donc pas un espace de non droit. Toutefois, compte tenu de la dimension transfrontalière et décentralisée du réseau, les protections réglementaires ne suffisent pas à instaurer un climat de confiance auprès des internautes. C'est pourquoi, en plus des normes légales, il est possible en tant que gestionnaires de site Web marchand de recourir à des garanties complémentaires.

## Les garanties complémentaires

Bien que certaines des garanties complémentaires soient déjà développées dans les chapitres précédents, il est intéressant de présenter les plus pertinentes, soit la sécurisation des transactions et des bases de données, les politiques relatives aux informations à caractère personnel, le standard P3P et les sceaux de certification.

### ► La sécurisation des transactions et des bases de données

La confiance et la sécurité sont les maîtres mots du développement d'Internet. En effet, pour pouvoir transmettre des données personnelles, les internautes doivent avoir le sentiment qu'aucun danger n'est à craindre, que le gestionnaire du site Web protège les informations tant au niveau de leur communication lors de la collecte que de leur stockage dans les bases de données.

La sécurité des transactions est essentiellement assurée par le recours à la cryptographie. Concrètement, dans le cadre d'un site Web marchand, lorsque le commerçant électronique veut collecter des renseignements personnels, il doit proposer une interface sécurisée. Par exemple, grâce au protocole SSL (Secure Socket Layers), les données saisies par l'internaute sont protégées et cryptées lors de leur transmission au serveur Web.

Une fois les informations transmises, le commerçant électronique doit également assurer la sécurité de sa base de données. En effet, seules les personnes autorisées doivent avoir la possibilité de consulter et de modifier lesdits renseignements. Les accès à la base de données doivent donc être restreints. En conséquence, le gestionnaire du site Web devrait prévoir deux types d'accès afin de garantir la protection des données. La première sera envisagée du côté du client, de l'internaute, la seconde du côté administratif, c'est-à-dire des personnes travaillant pour le compte du site Web marchand.

Du côté de l'internaute, le commerçant électronique doit lui donner le droit d'interroger la base de données afin de mettre à jour ses renseignements personnels, mais en aucun cas il

ne doit pouvoir modifier d'autres informations. Cette possibilité ne doit être accordée qu'aux administrateurs du site Web. Cela signifie que seules les personnes autorisées par le commerçant électronique peuvent accéder à l'intégralité de la base. Ces personnes sont dûment identifiées et pourront être tenues responsables des pertes, destructions ou utilisations illicites des renseignements personnels ainsi conservés. À cet égard, le commerçant devrait établir une politique interne de sécurité.

La sécurisation des transmissions et des bases de données constitue l'élément essentiel de la protection des renseignements personnels sur Internet. Le commerçant électronique peut vouloir aller plus loin en mettant en place des coupes-feux (*firewalls*), c'est-à-dire des barrières techniques permettant de protéger le serveur hébergeant le site Web marchand de toute intrusion extérieure et donc les informations qui y sont conservées.

En outre, le commerçant électronique aurait avantage à dégager sa responsabilité lors de transfert de documents ou de données via un forum de discussion dont il est le gestionnaire. En effet, il devrait indiquer à ses clients qu'ils doivent prendre toutes les mesures nécessaires pour assurer leur propre protection. S'agissant d'une aire publique, toute personne peut avoir accès aux données et ainsi les intercepter.

Enfin, le commerçant électronique devrait préciser qu'il n'est pas responsable de la politique relative aux renseignements personnels mise en place par les autres sites auxquels il est fait référence sur son site Web.

**► Les politiques relatives aux informations à caractère personnel**

Les politiques relatives aux informations à caractère personnel formalisent les engagements des commerçants électroniques envers les internautes. Toutefois, la mise en place de politiques n'exonère pas les sites Web marchands de leurs obligations légales.

L'élaboration de politiques se fait non seulement sur une base volontaire, mais aussi sans réel modèle. En effet, chaque commerçant électronique édicte sa propre politique selon ses besoins et prétentions. Cette dernière devrait non seulement être crédible, claire et compréhensible mais aussi accessible depuis la page principale du site Web, à défaut de l'être sur toutes les pages. Le commerçant électronique devrait y expliquer les points suivants :

- l'engagement en matière de renseignements personnels ;
- les informations collectées ;
- l'utilisation faite des informations ;
- le partage éventuel des informations ;
- l'utilisation des fichiers témoins et leur finalité ;
- l'existence d'un droit d'opposition à la diffusion de leurs renseignements et la manière de l'exercer ;
- l'existence d'un droit d'accès, de modification et de radiation de leurs renseignements et la manière de les exercer ;
- la sécurité du site Web ;
- les mentions légales à l'effet que le site Web est, si tel est le cas, assujetti à une législation nationale particulière, et
- le recours éventuel à un sceau de certification ou à un standard technique tel que le *Platform for Privacy Preferences Project* (P3P).

En somme, la politique indique aux consommateurs les engagements de l'entreprise relativement à la protection des renseignements personnels. Ainsi, pour connaître les prétentions des commerçants électroniques, les internautes doivent expressément consulter la politique lors de leur navigation. À cet égard, le projet de standard P3P vise à dévoiler les intentions du commerçant électronique dès que l'internaute saisi l'URL du site Web marchand.

**► Le *Platform for Privacy Preferences Project* ou P3P**

Le standard P3P, développé par le *World Wide Web Consortium* (W3C), permet l'établissement d'un dialogue entre les commerçants électroniques et les internautes relativement à la protection de leurs renseignements personnels.

En effet, le standard P3P permet aux commerçants électroniques de préciser leurs pratiques en matière de traitement des données personnelles. Ces spécifications sont formulées selon certains critères pouvant être interprétés automatiquement par les navigateurs des internautes. Ces critères font l'objet de préférences tant dans le logiciel de navigation que sur le serveur Web du site visité.

Ainsi, si les intentions du site Web en matière de collecte, d'utilisation des renseignements répondent aux attentes de l'internaute, ce dernier peut accéder audit site. Dans le cas contraire, l'internaute est informé des pratiques envisagées par le commerçant électronique. Il a le choix soit de naviguer sur le site Web en toute connaissance de cause, soit de mettre fin à sa visite.

L'efficacité de P3P repose sur l'établissement d'un dialogue entre le navigateur et le serveur. Ce dialogue est basé sur l'une ou plusieurs des catégories de données susceptibles de faire l'objet d'un traitement, à savoir :

- les informations permettant une prise de contact physique, comme le numéro de téléphone ou l'adresse postale ;
- les informations permettant une prise de contact électronique, comme le courriel ;
- les informations relatives à un identifiant unique, comme le numéro de sécurité sociale, d'assurance maladie ;
- les informations relatives à un identifiant financier, comme le numéro de carte de crédit, le numéro de compte bancaire ;
- les informations informatiques, comme l'adresse IP, le nom de domaine, le système d'exploitation utilisé ;
- les informations relatives à la navigation sur Internet, c'est-à-dire les pages précédemment consultées et la durée de cette visite ;
- les informations relatives à l'activité en ligne, c'est-à-dire les achats, les recherches effectuées ;
- les informations démographiques et socio-économiques, comme l'âge, le revenu ;
- les informations relatives aux préférences personnelles, comme les goûts musicaux ;
- les informations de communication, comme les expressions utilisées lors de vos échanges par courriel ou dans un groupe de discussion.

En utilisant le standard P3P, les commerçants électroniques et les internautes peuvent commercer sur la base d'un terrain d'entente en matière de traitement des données

personnelles. Il est donc important que les sites Web marchands prennent en considération ce projet qui favorise une interaction avec leurs consommateurs.

Toutefois, le fait de déclarer ses intentions en ce qui concerne les renseignements personnels des internautes ne doit pas exonérer le commerçant électronique de respecter ses engagements et de tout mettre en œuvre pour garantir la sécurité des informations qu'il détient. En effet, P3P énonce les pratiques des commerçants électroniques mais ne les certifie pas.

**► Les sceaux de certification des sites Web marchands**

La présence d'un logo, d'une griffe, d'un sceau fournit aux internautes l'assurance que le site Web marchand sur lequel ils naviguent respecte certaines conditions telles que la protection des données personnelles, la sécurité des transactions et l'observance de garanties légales ou complémentaires.

L'obtention d'un sceau se fait sur une base volontaire. En effet, rien n'oblige un commerçant électronique de certifier ses pratiques. Toutefois, le recours à un sceau de certification favorise l'établissement d'un rapport de confiance. Les organisations qui reviennent le plus souvent en matière de renseignements personnels sont *TRUSTe*, *BBBOnLine Privacy* et autres *Webtrust*, *BetterWeb*, etc.

Le certificateur TRUSTe est une organisation qui vise à promouvoir la confidentialité des informations détenues par un commerçant électronique. Pour devenir membre de cette organisation, les sites Web marchands doivent suivre trois étapes.

Tout d'abord, le commerçant électronique doit soumettre les principes qu'il s'engage à respecter en matière de renseignements personnels. Il peut soit déposer une politique existante, soit suivre le modèle établit par TRUSTe. Les règles mises en place par le commerçant électronique doivent tenir compte d'un certain nombre de points, à savoir :

- les renseignements collectés sur le site Web ;
- les méthodes de collecte des renseignement ;
- les personnes ou entreprises pour lesquelles les renseignements sont collectés ;
- l'utilisation particulière des renseignements ;
- les personnes ou entreprises avec lesquelles les renseignements sont partagés ;
- le choix de l'internaute en ce qui concerne la collecte, l'usage et l'échange des ses renseignements ;
- les moyens envisagés pour garantir la sécurité des renseignements, et
- le droit pour l'internaute de consulter, corriger et radier les renseignements détenus par le site Web.

Si la politique répond aux exigences de TRUSTe, le commerçant électronique doit ensuite faire parvenir à l'organisme une copie signée par laquelle il accepte les conditions d'adhésion au programme, ainsi que sa cotisation annuelle. Une fois les formalités et vérifications accomplies, TRUSTe délivre au commerçant électronique une licence. Cette dernière certifie que le site Web est membre de TRUSTe comme le prouve le sceau qui devra être apposé sur ledit site.

Cette procédure est également utilisée par le certificateur BBBOnLine. Dans ce cas, le commerçant électronique doit disposer d'une politique en matière de renseignements

personnels accessible sur son site Web. Il peut dès lors remplir une demande d'adhésion en fournissant des informations sur la compagnie et ses responsables, et notamment payer une cotisation et répondre aux questions relatives aux points suivants :

- les informations générales sur le site Web ;
- les informations sur la politique relative aux informations à caractère personnel ;
- les renseignements collectés ;
- le traitement des renseignements collectés ;
- le choix et le consentement de l'internaute ;
- la protection des renseignements ;
- l'accès aux renseignements ;
- l'accès du site par des enfants ;
- le consentement des parents ;
- l'existence ou non d'une politique concernant les enfants ;
- l'accès des parents ;
- les renseignements collectés au sujet des enfants ;
- les liens vers les autres sites.

Pour finir, le commerçant électronique doit retourner à l'organisation une copie signée en vertu de laquelle il accepte les conditions d'utilisation du sceau qui lui sera délivré et qu'il devra apposer sur son site Web.

## Conclusion

Sur Internet, la protection des renseignements à caractère personnel est un objectif que le commerçant électronique doit non seulement poursuivre mais aussi démontrer. La confiance est en effet l'élément-clef d'une relation commerciale souvent éloignée et ponctuelle. Dès lors, le commerçant électronique devrait clairement expliquer ses engagements en matière de renseignements personnels ainsi que la manière dont il entend garantir la confidentialité des données qu'il détient.