



**ASSOCIATION FRANCOPHONE DES AUTORITÉS DE PROTECTION  
DES DONNÉES PERSONNELLES (AFAPDP)**

**JOURNÉES DES RÉSEAUX INSTITUTIONNELS DE LA FRANCOPHONIE  
18 ET 19 MAI 2010**

**LA PROTECTION DES DROITS DANS UN CONTEXTE DE MONDIALISATION :  
Défis afférents à la protection des données personnelles pour la garantie  
des droits fondamentaux et la consolidation de la démocratie.**

Chers amis,

Je remercie la Délégation à la Paix, à la Démocratie et aux Droits de l'Homme de l'Organisation internationale de la Francophonie de me donner l'occasion de vous entretenir aujourd'hui des défis de plus en plus sérieux à l'égard de la protection des données personnelles. Nous verrons que ces défis peuvent être considérés au regard des principes énoncés dans la Déclaration de Bamako sur la garantie des droits fondamentaux et la consolidation de la démocratie.

Après une brève introduction concernant le droit fondamental à la protection des données à caractère personnel, je vous entretiendrai, comme le proposent les termes de référence, de l'expérience acquise à ce sujet, des résultats enregistrés et des difficultés auxquelles il faut maintenant s'attarder.

**1. LA PROTECTION DES DONNÉES PERSONNELLES**

Les données personnelles sont des renseignements qui concernent une personne physique et permettent de l'identifier.

Les États prescrivent la confidentialité de ces renseignements personnels. Au moment de la collecte, de l'utilisation, de la communication ou de la conservation, les données qui concernent une personne physique et permettent de l'identifier doivent être protégées. De plus, il est interdit aux organismes publics et aux entreprises de recueillir, utiliser, communiquer ou conserver des données à caractère personnel sans le consentement de la personne concernée, sauf si la législation d'un État le permet, dans un cadre défini.

Sur le plan national, la protection des données personnelles est assurée par un texte constitutionnel ou législatif garantissant la confidentialité. Les États confient la mise en œuvre de ces principes de protection de la vie privée à une autorité de contrôle indépendante qui doit exercer le suivi approprié.

Je dois rappeler que les règles élaborées par les États à ce sujet peuvent être différentes d'un pays ou d'un gouvernement à l'autre, tout comme les règles de mise en œuvre.

Sur le plan international, plusieurs documents juridiques importants ont été élaborés pour coordonner et unifier des règles de protection des données personnelles à l'égard d'un ensemble d'États ou de gouvernements. Par exemple, dès 1981, le Conseil de l'Europe a adopté la Convention 108 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Lors de l'assemblée générale du 14 décembre 1990, l'ONU a adopté la Résolution 45/95 concernant les principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel.

Le 24 octobre 1995, la Directive 95/46/CE du Parlement européen et du Conseil a été adoptée relativement à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.

On constate que de nombreux textes législatifs nationaux et différents documents internationaux prévoient des règles de protection des données à caractère personnel. Par contre, il n'existe actuellement aucun instrument juridique universel reconnaissant le droit fondamental à la confidentialité des données personnelles.

À ce stade, permettez-moi de rappeler que la protection des données personnelles contribue à la garantie des droits fondamentaux et à la consolidation de la démocratie, notamment lorsque les données personnelles concernent l'identité d'une personne physique.

En effet, la protection des données relatives à l'identité d'une personne lui garantit, notamment, le droit d'être reconnue à titre de citoyen, le droit de voter. De la même façon, cette personne peut alors exiger la reconnaissance de son droit à la sécurité, à l'éducation ou à la non-discrimination. En fait, la protection des données personnelles d'une personne physique contribue directement à la protection contre les abus, l'injustice et la discrimination.

Le souci de la garantie effective des droits fondamentaux des citoyens implique la mise en œuvre, par l'État concerné, de mesures de protection des données à caractère personnel.

## 2. EXPÉRIENCES ACQUISES

Dans un contexte traditionnel, la protection de la vie privée et des données personnelles se résume à la protection de la confidentialité des renseignements personnels conservés dans des dossiers physiques.

L'avènement des technologies de l'information a complètement changé la situation. Alors qu'il était autrefois possible de consulter les documents relatifs à la collecte, l'utilisation ou la communication de renseignements personnels, ce n'est plus le cas. Le traitement électronique des données à caractère personnel échappe au contrôle traditionnel des États et des gouvernements.

Les appareils technologiques et les applications qui sont introduits se développent à une vitesse fulgurante. Même les spécialistes peinent à prendre la mesure de toutes les conséquences de ces nouveaux instruments sur la protection des données personnelles. Le courrier électronique, Internet, les réseaux sociaux et les caméras de surveillance sont autant d'exemples de technologie de pointe qui permettent une intrusion, généralement non autorisée, dans la vie privée des utilisateurs.

Par exemple, le courrier électronique doit être comparé à une carte postale. Tout ce que nous écrivons par courrier électronique peut être intercepté et lu à notre insu. Les renseignements que nous plaçons dans les réseaux sociaux sont accessibles à un très grand nombre de personnes, comme s'ils étaient affichés dans un endroit public, sans que nous soyons informés de l'identité des personnes qui en prennent connaissance. En plus, ces renseignements sont généralement conservés indéfiniment.

Les exemples ne cessent de se multiplier concernant des situations où des renseignements personnels ont été utilisés à des fins illicites, grâce aux technologies de l'information. Ces utilisations illicites ont entraîné des conséquences personnelles et financières très sérieuses dans de nombreux cas. On compte aussi des exemples de personnes qui ont tenté d'attenter à leur vie à la suite de propos ou d'images diffamatoires publiées à leur égard, sans leur consentement.

Malgré ces risques, la popularité de ces instruments électroniques ne cesse de croître alors que les États et gouvernements devant la rapidité de ce développement, ne sont pas prêts à y faire face, tant sur le plan législatif que dans la mise en œuvre des moyens de contrôle.

Les développements technologiques actuels présentent d'autant plus de difficultés qu'ils s'effectuent bien au-delà des frontières traditionnelles. Le réseau technologique mondial a été construit sans égard aux frontières des États. Il s'en

suit que les données personnelles d'un citoyen européen peuvent être conservées en Asie ou en Amérique du Sud, par exemple. On imagine alors la difficulté d'exercer un contrôle effectif sur la protection des renseignements personnels conservés à l'extérieur de l'Europe.

Sur le plan du droit international, l'autorité de chacun des États s'exerce à l'intérieur des frontières, sous réserve des engagements pris dans le cadre de différents instruments internationaux auxquels des États ont souscrit.

Comme je le mentionnais plus tôt, ce ne sont pas tous les États et gouvernements qui, jusqu'à maintenant, ont introduit des législations relatives à la protection des données personnelles et mis en place une autorité indépendante de contrôle. Non seulement ce ne sont pas tous les États qui ont adopté les législations requises mais également lorsque des législations existent, les normes peuvent varier d'un pays ou d'un gouvernement à l'autre.

Nous sommes ainsi en présence d'une difficulté majeure pour exercer une vigilance et un contrôle adéquat de la protection des données personnelles des individus au-delà des frontières des États. Cette difficulté d'exercer un contrôle effectif au-delà des frontières, plus spécialement sur le plan technologique, fragilise de façon correspondante la protection des données à caractère personnel des individus. Cette difficulté se transpose dangereusement sur la garantie des droits fondamentaux des individus.

### **3. CERTAINS RÉSULTATS ENREGISTRÉS EN FRANCOPHONIE**

Dans l'objectif de tenter d'exercer un contrôle effectif au-delà des frontières, plusieurs pays ayant en partage le français ont, depuis plus de cinq ans, réuni leurs efforts afin, notamment, de coordonner la mise en œuvre de la protection des données à caractère personnel. Ces efforts ont été plus spécialement concrétisés à l'occasion d'une réunion de travail tenue à Monaco en septembre 2006. Les représentants de onze États et gouvernements ayant en partage le français ont convenu d'établir les bases d'une association des autorités indépendantes de protection des données personnelles de la Francophonie. Les participants ont également souhaité collaborer à l'élaboration d'un texte juridique d'application universelle relatif à des principes de protection des données à caractère personnel.

Les engagements convenus à l'occasion de cette rencontre de septembre 2006 ont été consignés dans la Déclaration de Monaco.

En septembre 2007, les représentants de plus de vingt pays ayant en partage le français se sont réunis à Montréal, à l'occasion de la première Conférence des commissaires à la protection des données de la Francophonie. Cette conférence fut consacrée à la promotion et la mise en œuvre du droit

fondamental à la protection des données à caractère personnel au sein de la Francophonie.

Au terme de la réunion, l'Association des autorités de protection des données personnelles fut constituée. Comme l'exprime le préambule des statuts de cette nouvelle association, la création d'un nouveau réseau institutionnel pour soutenir la protection des données à caractère personnel, doit permettre de donner suite aux principes de protection des droits fondamentaux énoncés dans la Déclaration de Bamako, repris dans les déclarations de Ouagadougou et de Bucarest.

Les États et gouvernements, ayant en partage le français, réunis à Montréal en septembre 2007, ont adopté la Déclaration de Montréal qui annonce la création de la nouvelle Association francophone des autorités de protection des données personnelles (AFAPDP) et réitère les objectifs fondamentaux de coopération et de développement des autorités indépendantes de protection des données personnelles au sein de la Francophonie.

Les déclarations de Monaco et de Montréal sont deux exemples importants des résultats enregistrés en Francophonie à l'égard de la protection des données à caractère personnel. Toutefois, les résultats enregistrés ne s'arrêtent pas là.

Depuis 2007, l'AFAPDP se réjouit d'une participation importante des pays et gouvernements francophones, plus spécialement au niveau des efforts pour promouvoir un instrument international. En fait, les pays et gouvernements intéressés participent de façon spontanée, soutenue et généreuse, dans l'objectif de promouvoir le droit fondamental à la protection des données à caractère personnel.

En pratique, les pays et gouvernements concernés partagent leurs expertises par des échanges, diffusent la documentation pertinente au bénéfice de tous les membres et offrent aux membres intéressés la possibilité d'effectuer un stage auprès d'une autorité de contrôle de la protection des données personnelles de la Francophonie.

L'AFAPDP a également, au cours des années, participé à des rencontres avec les autres réseaux institutionnels de la Francophonie, notamment sous le thème de la responsabilité sociale des entreprises et sur celui des modes de financement européens.

Plus récemment, l'AFAPDP s'est associée à l'Association des Ombudsmans et Médiateurs de la Francophonie (AOMF), dans un projet commun relatif à la promotion et la protection des droits des enfants, notamment la protection de leurs données à caractère personnel.

Enfin, depuis plus de deux ans, l'Association francophone des autorités de protection des données personnelles (AFAPDP) s'est vue reconnaître un statut d'observateur au sein du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), du Conseil de l'Europe. Plus récemment, le T-PD Bureau a préparé une recommandation à l'intention du Conseil de l'Europe concernant la gestion électronique des données dans un contexte de profilage des individus auquel a contribué l'AFAPDP.

#### **4. DIFFICULTÉS RESTANTES À SURMONTER**

##### **Difficultés restantes**

Les principes fondamentaux de protection des données à caractère personnel que l'on croyait reconnus et acceptés font encore l'objet d'attaques sérieuses.

Plus spécialement depuis septembre 2001, plusieurs États et gouvernements prétendent qu'il est nécessaire, pour des motifs de sécurité, de faire exception à la confidentialité des données à caractère personnel, lorsque des questions de sécurité sont en jeu. L'équilibre entre les deux objectifs doit être maintenu en exerçant un suivi attentif pour éviter d'écarter précipitamment la protection de la vie privée.

Plusieurs grandes entreprises technologiques qui œuvrent dans Internet, cherchent, de leur côté, à convaincre la population que les renseignements versés dans Internet par un citoyen ne sont pas confidentiels. Ce dernier aurait renoncé à la confidentialité en plaçant ses informations dans Internet.

La plupart du temps, cette circulation des données à caractère personnel s'effectue à l'insu de la personne concernée. Il ne lui est pas possible de connaître tous les endroits où circulent ses renseignements personnels dans Internet. Face à l'impossibilité d'exercer un suivi approprié de la communication incontrôlée de leurs renseignements personnels les citoyens semblent choisir de baisser les bras, pour s'en remettre totalement aux fournisseurs.

En fait, nous constatons qu'une mauvaise compréhension des principes de protection des données à caractère personnel, plus spécialement des risques dans Internet, contribue à l'inaction des internautes.

En l'absence de principes de protection des données à caractère personnel reconnus et appliqués universellement, le développement fulgurant des applications disponibles dans Internet ainsi que la participation massive aux nombreuses activités disponibles sur le Web, constituent un phénomène puissant et incontournable. Il risque de compromettre définitivement la mise en

œuvre des règles de protection des données à caractère personnel, au péril de la démocratie.

### **Action des membres de l'AFAPDP**

Loin de baisser les bras, les membres de l'AFAPDP, comme je le mentionnais précédemment, ont déjà entrepris plusieurs actions visant à défendre et promouvoir la protection des données à caractère personnel.

Au niveau international, les démarches de l'AFAPDP comprennent un appui à l'élaboration d'un cadre normatif conforme et cohérent avec les principes législatifs déjà reconnus dans plusieurs États en matière de protection des données à caractère personnel.

Les membres de l'AFAPDP apportent également un appui inconditionnel à la mise en œuvre d'une législation nouvellement adoptée dans un pays de la Francophonie et à la mise en place d'une autorité indépendante de contrôle. Cet appui se traduit notamment par une offre de stages individuels ou collectifs.

L'AFAPDP participe aux travaux d'un groupe francophone de réflexion sur l'établissement d'un instrument international sur la protection des données personnelles et de la vie privée. Le groupe de réflexion OIF-AFAPDP est présidé par le président de l'AFAPDP. Ce groupe doit produire un rapport concernant la pertinence d'élaborer un instrument international en matière de protection des données à caractère personnel, de recommander l'utilisation d'un instrument international déjà existant ou de faire des recommandations concernant la mise en œuvre de ces principes sur le plan international.

## **5. CONCLUSION**

La protection des données à caractère personnel est indispensable à la garantie des droits fondamentaux et à la consolidation de la démocratie.

Sans nous soucier des risques, nous versons dans Internet de plus en plus d'information nous concernant, parfois des renseignements très confidentiels. Grâce à des outils technologiques très puissants, à une capacité de stockage des données presque illimitée, les criminels sont de plus en plus en mesure de connaître beaucoup de choses sur chacun d'entre nous, et même de nous attribuer un profil. Non seulement les développements technologiques permettent aux criminels d'effectuer des recherches et de recueillir les données correspondantes, mais également ils font perdre aux citoyens le droit à l'oubli puisque les données versées dans Internet peuvent être conservées à tout jamais, à notre insu.

Les personnes ou les entreprises, qui effectuent l'analyse des informations nous concernant, disponibles dans Internet, prétendent qu'elles peuvent, de cette façon, tout savoir sur nous. Toutefois, l'exactitude de l'information placée dans Internet à notre sujet, parfois par des inconnus, n'est pas vérifiée, ni validée et présente des risques majeurs de nuire à la personne concernée, alors qu'elle n'est pas prévenue.

En effet, l'internaute ne peut pas savoir qu'elles sont les informations qui ont été conservées à son sujet. Non seulement il ne peut pas savoir ce que l'on sait sur lui, mais en plus il ne peut pas vérifier, notamment pour se prémunir des conséquences très négatives d'une information inexacte consignée à son dossier. Plus spécialement pour les données stockées à l'extérieur des frontières nationales, l'internaute ne dispose pas de recours effectifs lorsqu'il est victime d'une inscription erronée dans Internet. L'absence de recours place le citoyen dans une situation où la garantie de ses droits fondamentaux, notamment celui relatif à la protection des données à caractère personnel, n'est pas respecté.

Je sou mets le tout à votre considération et vous remercie de votre attention.

Jacques Saint-Laurent  
Président de L'Association francophone des autorités de protection des données  
personnelles (AFAPDP)  
Président de la Commission d'accès à l'information du Québec