Date : 02/08/2008

RELU PAR LE CFI

Document de réflexion sur les dimensions éthique, juridique et politique de la gestion des données à caractère personnel

Dr. J. Eric Davies
Honorary Visiting Research Fellow
Department of Information Science,
Loughborough University. Loughborough. LE11 3TU. UK.
Email: j.e.davies@lboro.ac.uk

***Traduit** par Claire TRANNE*
Université Lyon 2, France
juillet 2008

Meeting: 165 Government Libraries
Simultaneous Interpretation: Not available

WORLD LIBRARY AND INFORMATION CONGRESS: 74TH IFLA GENERAL CONFERENCE AND COUNCIL
10-14 August 2008, Québec, Canada
http://www.ifla.org/IV/ifla74/index.htm

Introduction

Dans nos sociétés modernes, la gestion des données à caractère personnel présente de nombreux défis sur le plan éthique, juridique et politique. La nécessité de respecter les données sur les personnes a été reconnue par de nombreux corps législatifs et est intégrée dans des traités internationaux. Ce document traite des quelques problèmes généraux soulevés et porte plus particulièrement sur le respect de la vie privée. Il s'inspire de manière générale, mais pas exclusivement, des orientations du Royaume-Uni et de l'Union Européenne. L'assurance d'un bon fonctionnement des sociétés du savoir en termes de politique et d'action repose sur un équilibre fragile entre ses besoins et le droit de chacun à la vie privée. Il ne s'agit pas d'un simple exercice philosophique puisque l'identification de la clé de voûte de cet équilibre a des implications importantes sur la manière dont les gouvernements et les activités sont menés et sur la façon dont les gens perçoivent la société dans laquelle ils vivent. Les gestionnaires de bibliothèque et de l'information sont confrontés aux défis que présentent ces problèmes et les prestations de service doivent être assurées de manière appropriée, eu égard à la vie privée. Le thème sous-jacent traité au travers de ce document est le devenir de l'individu en tant que citoyen (notamment en tant qu'usager des services de bibliothèque et de l'information) dans l'univers de l'information.

Analyse de la vie privée

Chaque fois que la dimension éthique de la gestion des données à caractère personnel est mise en cause et indépendamment du lieu, le concept de la vie privée apparaît comme un facteur-clé qui détermine les dimensions et les frontières d'une activité, à la fois sur le plan pratique et politique. Mais qu'est-ce exactement que la vie privée et, en tant que droit dans les sociétés libres, quelles sont ses limites ?

Le *Oxford English Dictionary* définit la « vie privée » comme :

> … le fait d'être seul, tranquille et loin de l'attention du public, résultant d'un choix ou d'un droit ; liberté qui découle de l'absence d'immixtion ou d'intrusion.

La notion de vie privée comme une chose que l'on jouit, entretient et protège en conséquence, prédomine dans de nombreux contextes et cultures et se trouve confortée dans des forums internationaux. La *Déclaration universelle des droits de l'homme*[1] des Nations Unies stipule, dans son article 12, un droit universel à la vie privée :

> Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

De même, le Conseil de l'Europe proclame dans la *Convention européenne pour la protection des droits de l'homme*[2] que :

> Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

Légiférer sur la protection de la vie privée n'a pas toujours été une tâche facile. Il est parfois difficile de parvenir à un consensus sur la nature et l'étendue de la protection requise. Il y a plus de trente-cinq ans, au Royaume-Uni, le Comité présidé par Younger sur la protection de la vie privée a fait observer dans son rapport[3] :

> Le concept de vie privée est relativement simple pour un citoyen ordinaire. Celui-ci peut facilement identifier la sphère de sa vie qu'il estime être sienne tout particulièrement et pour laquelle il réclame le droit d'être protégé contre l'immixtion extérieure ou les publicités indésirables. Néanmoins, l'importance que l'on attache à la vie privée selon sa forme et les intrusions contre lesquelles une protection est recherchée diffèrent si fortement d'un individu à l'autre et d'une catégorie à l'autre, qu'il est difficile jusqu'ici de placer le concept clairement dans un cadre juridique unique afin que, dans l'ensemble, il soit raisonnablement reconnu et protégé dans le droit civil et pénal.

La vie privée peut être protégée par une législation connexe relative à la violation de propriété ou la violation de l'obligation de confidentialité, mais certains pays ont des lois spécifiques sur la protection de la vie privée. Par exemple, les Etats-Unis[4] et le Canada[5] ont une législation qui étaye le respect de la vie privée en ce qui concerne les données à caractère personnel détenues par les institutions gouvernementales. La vie privée figure également dans des dispositifs semi-formels mais généralement efficaces, tels que ceux du Comité d'examen des plaintes concernant la presse[6] (*Press Complaints Commission*) dont l'objet et de servir de garde-fous contre l'intrusion excessive de la presse et des média dans la vie des personnes.

---

[1] UNITED NATIONS. Universal Declaration of Human Rights.[Article 12]. New York, U.N., 1948.
[2] COUNCIL of EUROPE. European Convention for the Protection of Human Rights and Fundamental Freedoms.[Article 8; Section 1]. Strasbourg, Council of Europe, 1950.
[3] GREAT BRITAIN. Committee on Privacy. *Report.*.. London, HMSO, 1972. (Command Paper: Cmnd 5012) (Chairman: Kenneth Younger)
[4] UNITED STATES Laws, Statutes. *Privacy Act.* 1974 (as amended)
http://opm.gov/feddata/USC552a.txt
[5] CANADA. Laws, Statutes. *Privacy Act.* 1985 (as amended)
http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-21///en
[6] PRESS COMPLAINTS COMMISSION. *Editors Code of Practice*. London, PCC, 2007.
http://www.pcc.org.uk/assets/111/Code_Aug_2007.pdf

Si l'on s'accorde sur le fait que l'atteinte à l'intimité de la vie privée d'une personne de façon arbitraire et abusive doit être condamnée, il est de plus en plus difficile pour une personne de garder sa vie dans le secret absolu tout en étant un membre actif de la société, en particulier au XXI^{e} siècle. Les mécanismes de la vie dans une société moderne, et plus précisément dans une société du savoir, impliquent un certain niveau de partage de données pour qu'elle puisse un tant soit peu fonctionner efficacement. En résumé, pour le bon fonctionnement d'une société, on s'accorde sur la nécessité que des données pertinentes et satisfaisantes soient disponibles. Ainsi, il faut souvent trouver un équilibre entre le droit au respect de la vie privée et le besoin de savoir de diverses agences. Il s'ensuit que, si les gens devaient garder confiance dans les organisations et leurs systèmes, des garde-fous sont nécessaires contre l'usage abusif de ce besoin de savoir et des données à caractère personnel qui s'y rattachent. De plus, il existe un impératif de transparence dans l'usage que font les agences des données à caractère personnel. Dans le même temps, les individus doivent être conscients aussi bien des risques que des avantages du partage des données à caractère personnel. Des comptes rendus récents[7,8] sur les sites de réseautage social, par exemple, laissent entrevoir l'indifférence alarmante ou, au mieux, l'inconscience de certaines personnes face aux dangers.

Technologie et vie privée

La technologie n'a de cesse d'ajouter de nouvelles dimensions aux méthodes de collecte, de stockage et d'usage de données à caractère personnel. En outre, elle a mis davantage en relief les dimensions éthique, juridique et politique de ces activités.

Il y a plus de trente ans, la possibilité et l'éventualité que des traitements de données de masse portent atteinte à l'intimité de la vie privée et aux intérêts des personnes constituaient déjà un sujet de préoccupation courant. Un document émanant du gouvernement du Royaume-Uni, apparu en 1975, résumait clairement les inquiétudes qui prédominaient :

> Qu'est-ce que les ordinateurs ont de spécial ?
>
> Aucune des fonctions exécutées par les ordinateurs au sein des systèmes d'information ne diffère en nature de celles qui sont réalisées, ou pouvaient en principe l'être, par des méthodes traditionnelles. Mais des différences importantes existent dans la façon et la rapidité avec lesquelles ces fonctions peuvent être réalisées par des systèmes informatiques d'une part, et par des systèmes traditionnels d'autre part.
> La vitesse des ordinateurs, leur capacité à stocker, associer, extraire et transférer des données, leur flexibilité et le faible coût unitaire du travail qu'ils peuvent effectuer ont dans la pratique des implications suivantes sur la vie privée :
> (1) ils facilitent l'entretien d'importants systèmes d'archivage et le maintien des données dans ces systèmes ;
> (2) ils rendent les données facilement et rapidement accessibles sur des lieux éloignés ;
> (3) ils rendent possible le transfert rapide des données d'un système d'information à un autre ;
> (4) ils permettent d'associer les données, ce qui n'aurait pas été possible autrement ;
> (5) parce que les données sont stockées, traitées et souvent transmises dans une forme qui n'est pas intelligible de prime abord, peu de gens sont susceptibles de connaître le contenu des fichiers ou de savoir ce qu'il advient de ceux-ci.[9]

La technologie du XXI^{e} siècle s'étend bien au-delà de ce que l'on imaginait en 1975. Pour commencer, l'accessibilité aux technologies de l'information et leur puissance se sont accrus de façon spectaculaire, de sorte que, dans le monde développé, il est presque commun de posséder un PC ou d'accéder aux réseaux. L'Internet permet aux données de faire le tour du monde à la vitesse de la lumière et aux systèmes considérablement éloignés de se connecter pour créer un environnement informatique généralisé.

[7] Davies, G. *Data Protection Topline Report.* Wilmslow, Information Commissioner's Office, 2007. http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/research_results_topline_report.pdf
[8] New front in the battle against identity theft. *The Independent.* 23 November 2007.
[9] GREAT BRITAIN. Home Office. *Computers and Privacy*. London, HMSO, 1975. (Command Paper: Cmnd. 6353)

L'ordinateur portable avec réseau sans fil confère une portabilité remarquable au stockage, au traitement et à la connectivité des données. Le téléphone portable est devenu presque universel et avec lui, le concept de partage et d'échange non seulement verbaux mais également textuels ou par images.

De plus, les techniques de capture de données s'étendent maintenant jusque dans l'univers de l'imagerie par satellite d'une part, et jusqu'aux confins de l'identification par l'iris d'autre part. Les données recueillies comprennent aussi bien des images et des sons provenant de la rue en temps réel, des profils ADN, des messageries vocales que des textes traditionnels et des faits. De plus, la remarquable croissance des capacités de stockage et celles de traitement se conjuguent pour donner de nouvelles dimensions au potentiel de l'exploration des données. Dans son nouveau livre, Ayres aborde et illustre cette tendance.[10] La loi de Moore, très souvent évoquée, selon laquelle la performance des microprocesseurs doublerait tous les deux ans concorde avec un phénomène tout aussi significatif et impressionnant concernant les densités de stockage de données. La loi de Kryder postule que les capacités de stockage des disques durs doubleraient tous les deux ans et qu'en outre le coût par gigaoctet serait également en baisse.[11] Dans les deux cas, il existe des implications profondes dans le fait que l'on puisse tirer une nouvelle signification des informations en tout genre, notamment des données à caractère personnel.

Les attitudes et les habitudes ont égalent évolué en matière d'usage de données à caractère personnel et de technologies de l'information, peut-être dans l'indifférence ou l'inconscience des implications d'une divulgation si aisée de données. Comme nous l'avons déjà évoqué, les sites Internet de réseautage social favorisent la divulgation et l'échange de données à caractère personnel et éprouvent par des procédés nouveaux les limites de la vie privée. A mesure que les transactions gouvernementales, bancaires et commerciales en ligne s'intensifient, les individus sont d'autant plus disposés à livrer des informations les concernant. Des millions de consommateurs fournissent au quotidien, et sans contrainte semble-t-il, divers renseignements concernant leurs dépenses personnelles par le truchement des cartes de fidélité de supermarché qui donnent des avantages relatifs en retour. Au résultat, une ambivalence de la vie privée semble actuellement se développer, dans laquelle les individus sont disposés à livrer certaines informations librement tandis que, dans le même temps, ils expriment leur inquiétude concernant les renseignements que l'on dispose sur eux et la façon dont ceux-ci sont utilisés. Un autre symptôme des inquiétudes concernant la vie privée, qui peut être révélateur, est le nombre de déchiqueteuses à usage domestique qui sont vendues à l'heure actuelle.

Tous ces facteurs concourent à remettre en cause l'usage des données à caractère personnel. Néanmoins, pour que la technologie ne soit pas stigmatisée trop emphatiquement, il est bon d'observer ce que dit très justement Michael Gorman dans son livre intitulé : *Our Enduring Values: Librarianship in the 21st Century* :

> Précisément, ce n'est pas la technologie qui est l'ennemi de la vie privée mais cette façon joyeuse que nous avons d'utiliser la technologie.[12]

Protection des données à caractère personnel

Le moyen le plus efficace de garantir un traitement adéquat des données à caractère personnel est la création d'un régime dans lequel l'action menée est exposée et transparente, et l'usage de l'information

[10] Ayres, Ian. *Supercrunchers: How anything can be predicted*. London, John Murray, 2007.
[11] Walter, C. Kryder's Law. *Scientific American.* 293 (2) July 2005. pp. 32-33.
[12] Gorman, Michael. *Our Enduring Values: Librarianship in the 21st Century*. Chicago, American Library Association, 2000. (Chapter 10 - Privacy. pp.144 – 157.)

susceptible d'être remis en cause. Une telle approche doit être étayée par une législation pour garantir son efficacité. De nombreux pays ont à l'heure actuelle une législation et des mécanismes bien en place pour veiller à ce que des données à caractère personnel soient traitées de manière responsable aussi bien par le secteur privé que public. Cela implique non seulement que la vie privée des individus soit respectée mais également que les données soient fiables et utilisées de manière adéquate.

C'est à la Hesse, en Allemagne, que l'on doit le tout premier énoncé de loi sur la protection des données en 1970. Par la suite, de nombreuses nations ont adopté une législation. Le Conseil de l'Europe tout comme l'Organisation de coopération et de développement économiques ont contribué à encourager chaque état à adopter des mesures de protection des données. L'un par un traité[13] soumis à la signature en 1981 et l'autre par un ensemble de lignes directrices[14] publiées la même année. Leur intérêt reflète aussi bien les implications commerciales d'un flux de données transfrontière efficace dans une économie mondiale du savoir que la protection de la vie privée. La nécessité d'harmoniser les diverses mesures en vigueur au sein des pays membres a conduit l'Union Européenne[15] à diffuser une directive en 1995, qui a servi de référence en matière de législation. Ses objets, comme stipulés dans l'article 1, porte sur la libre circulation des données entre états membres d'une part et les droits fondamentaux et les libertés des individus d'autre part :

Article 1 Objet de la directive

1. Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

2. Les États membres ne peuvent restreindre ni interdire la libre circulation des données à caractère personnel entre États membres pour des raisons relatives à la protection assurée en vertu du paragraphe 1.

Cette directive sert de fondement à la législation actuelle sur la protection des données au Royaume-Uni, adoptée en 1998. La Loi sur la protection des données[16] (*Data Protection Act*) est ainsi définie dans son préambule :

Une loi qui tient lieu de nouvelle disposition pour la régulation des traitements des données relatives aux personnes, notamment l'obtention, la détention, l'utilisation ou la divulgation de ces données.

Cette loi précise les activités acceptables et instaure un système de surveillance et de régulation de l'usage des données à caractère personnel. Elle s'applique aux données à caractère personnel dans toutes ses formes : analogique, digital, textes, images et sons. Les activités acceptables sont définies au travers d'une série de principes généraux à suivre lorsque celles-ci mettent en jeu des données à caractère personnel. Pour résumer rapidement, les données à caractère personnel doivent être :

- traitées correctement et conformément au droit
- obtenues et traitées uniquement à des fins définies et légales

[13] COUNCIL OF EUROPE. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Strasbourg, Council of Europe, 1981. (European Treaty Series No. 108)
[14] ORGANISATION for ECONOMIC CO-OPERATION and DEVELOPMENT. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Paris, OECD, 1981.
[15] EUROPEAN UNION. Directive 95/46/CE du Parlement et Conseil des Communautés européennes du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**.** JOCE, n° L. 281/31 du 23 novembre 1995. Brussels, E.U., 1995. (In: Official Journal of the E.U. Part (L), 23rd Nov. 1995, p.31).
[16] GREAT BRITAIN.Laws, Statutes. *The Data Protection Act.* (Public General Acts 1998 - Chapter 29). London, SO, 1998.

- correctes, pertinentes et pas excessives
- précises, et si nécessaire, mises à jour
- ne pas être conservées au-delà du temps nécessaire
- traitées conformément aux droits des personnes auxquelles les données se rapportent
- traitées avec des mesures de sécurité adaptées sur le plan technique et organisationnel
- ne pas être transférées dans un pays ou territoire en dehors de l'Espace économique européen à moins que ce pays ou ce territoire assure un niveau adéquat de protection de données.

La surveillance et la régulation des activités relèvent de la responsabilité du commissaire à l'information qui a le pouvoir d'identifier, de consigner, d'approuver et de diriger les activités des usagers des données en se référant aux principes en question et à la loi. Il existe également un tribunal de protection de données pour instruire les appels contre les décisions du commissaire. Un Registre des usagers des données est conservé et les individus ont la possibilité de donner leur consentement éclairé aux traitements des données et ont accès à celles-ci, en d'autres termes, ils peuvent attester des données les concernant et consulter un exemplaire de tout élément d'information détenu. Il existe quelques dérogations au respect de toutes les conditions spécifiées dans la législation, notamment : les éléments d'information utilisés dans la protection de la sécurité nationale, la prévention et la détection des crimes et les traitements de données « modestes » à usage domestique. Le texte intégral est disponible sur le Web à l'adresse :
http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm

La législation fonctionne assez bien et le commissaire semble assez vigilant en ce qui concerne l'utilisation des données à caractère personnel au Royaume-Uni aussi bien dans le secteur public que privé. Le commissaire a fait des observations formelles sur les projets du gouvernement du Royaume-Uni concernant l'introduction des cartes d'identité et a précisé la nécessité de mettre en place des garde-fous adaptés.[17] Il a également examiné de près des cas récents de perte de données par des agences gouvernementaux.

Il est à noter qu'une des conditions de la législation établie dans l'Union européenne est que les données ne puissent pas être transférées dans un pays ou territoire en dehors de l'Espace économique européen à moins que ce pays ou ce territoire assure un niveau de protection de données adéquat. Pendant un certain temps, l'échange de données entre les Etats-Unis et l'Europe a soulevé des inquiétudes. La démarche de protection de données aux Etats-Unis est quelque peu différente et manque d'adéquation avec ce qui se pratique en Europe. Le problème a été finalement résolu avec la mise en place de l'accord *Safe Harbor*, aux termes desquels les organisations aux Etats-Unis sont dûment reconnues en matière d'échange de données à caractère personnel.[18]

L'individu en tant que citoyen

Comme nous l'avons fait observer, dans une société moderne du savoir, il faut un certain degré de communication et d'échange, sinon de mise en commun de données à caractère personnel, si cette société devait mener ses activités de manière efficace, économique et effective. Prenons un cadre contextuel pour illustrer nos propos : les gouvernements fonctionnent sur cette base en termes de politiques, de planifications et d'administration et ils agissent ainsi depuis un certain temps. Au Royaume-Uni, par

[17] GREAT BRITAIN. Information Commissioner. *Identity Cards Web Page.* (Accessed: April 2008.) http://www.ico.gov.uk/Home/about_us/news_and_views/current_topics/identity_cards.aspx
[18] UNITED STATES. Department of Commerce. *Safe Harbor Workbook.* Washington, US DoC, 2005 http://www.export.gov/safeHarbor/sh_workbook.html

exemple, le premier recensement moderne et officiel de la population sur le plan national a été entrepris en 1801, et le premier dans lequel les noms ont été enregistrés a eu lieu en 1841. Les évolutions en matière d'aides sociales ou de prospérité économique seraient minimes sans une vue d'ensemble suffisamment précise et détaillée de la situation démographique du pays.

De nos jours, il n'y a que le volume d'informations réunies qui a changé, et la façon dont elles sont ou peuvent être traitées, distribuées et utilisées au moyen des technologies de l'information. Les ambitions du gouvernement du Royaume-Uni concernant l'application des technologies dans l'administration en ligne sont bien documentées [19,20,21,22]. La plupart d'entre elles sont menées à bien en mettant en relation le citoyen avec les administrations locales ou nationales. Cependant, ces développements soulèvent des inquiétudes sur l'équilibre, voire la tension, qui existe entre le droit de l'individu à l'intimité de la vie privée et le besoin de la nation de savoir, mais aussi sur la sécurité intrinsèque qui entoure ces informations. Si l'assimilation de toute société démocratique moderne au scénario dépeint dans le livre 1984 d'Orwell pourrait être taxée d'extravagance, certains peuvent émettre des doutes devant la visible montée en puissance de l'Etat et ses traitements de données. Des controverses récentes au Royaume-Uni concernant la proposition d'introduction de cartes d'identité digitales en est un exemple. Des cas de pertes de données, qui ont été fortement médiatisés, et des révélations des agences gouvernementales ajoutent à l'inquiétude et n'inspirent pas confiance chez tout un chacun quant à la gestion de l'information par l'Etat et le respect de celui-ci de la vie privée.

La relation existant entre l'individu en tant que citoyen et l'Etat en tant qu'agent peut être perçue dans le cadre de l'usage de l'information dans des applications diverses, notamment : la planification économique, la santé publique, l'éducation, l'aide sociale, la cohésion sociale, l'application de la loi, la prévention contre le crime, et plus récemment les contre-mesures dans le terrorisme. Ainsi, une pléthore d'informations stratégiques est requise sur la population, l'emploi, la migration, la maladie et la mortalité, les compétences et l'acquisition des connaissances, le manque de contacts sociaux ainsi que les actes criminels et les peines. La plupart de ces informations sont utiles et utilisables à un niveau « macro » généralisé. Part ailleurs, les transactions et les interactions entre le citoyen et l'Etat doivent nécessairement être établies à un niveau plus individuel où l'assurance identité est essentielle et les données à caractère personnel sont obligatoirement communiquées. Dans ce contexte, la sécurité et l'intégrité des données ainsi que son utilisation adéquate prennent plus d'importance. Il est possible que l'Etat ait besoin de connaître l'état de santé d'un individu, son origine ethnique, sa situation financière, ses charges familiales et même son casier judiciaire, mais aussi de données plus communes comme l'adresse, l'âge et le sexe. Dans certains cas, un mélange complexe d'informations est utilisé, ce qu'illustrent le péage routier et le péage urbain qui impliquent de localiser sur une carte un véhicule (et son propriétaire ou conducteur) en temps réel et le relier à des bases de données de paiements et d'identité.

La prévention contre les actes criminels et sa détection, et tout particulièrement la lutte contre le terrorisme, reposent sur une importante collecte d'informations et surveillance et, lorsque celle-ci est nécessaire et autorisée, l'interception des communications. Le rassemblement de ces données peut porter atteinte aux intérêts légitimes d'une personne qui respecte la loi et constitue ainsi un sujet de

[19] GREAT BRITAIN. Cabinet Office. *Modernising Government.* London, SO, 1999. (Command Paper: Cm 4310) (Chapter 5 - Information Age Government)
[20] GREAT BRITAIN. Cabinet Office. *Transformational Government Enabled by Technology*. London,SO, 2005. (Command Paper: Cm 6683)
[21] Mayo, E. and Steinberg, T. *The Power of Information: An independent review*. London, Cabinet Office, 2007.
[22] GREAT BRITAIN. Cabinet Office. The Government's Response to: The Power of Information: An independent review. London, SO, 2007. (Command Paper: Cm 7157)

préoccupation. L'adage selon lequel : « …ceux qui n'ont rien à cacher n'ont rien à craindre… » sonne parfois creux à la lumière des risques d'inexactitude, de perte ou d'utilisation abusive de ces données. Le commissaire à l'information[23] dans une communication adressée au Parlement signale les risques :

Les risques qui résultent d'une surveillance excessive nous affectent sur le plan individuel et affectent la société dans son ensemble. L'immixtion excessive dans la vie des gens peuvent se traduire par des usages à leur insu, qui présentent un caractère inacceptable et préjudiciable. Les erreurs peuvent être faites et des inexactitudes peuvent survenir, perturbant ainsi la vie quotidienne des individus dans la mesure où une confiance accrue est placée sur un seul rassemblement centralisé de données à caractère personnel…

Pour les individus, le risque est qu'ils pourront être lésés lorsque les données les concernant sont :

- inexactes, insuffisantes ou désuètes ;
- excessives ou inadéquates ;
- gardées trop longtemps ;
- communiquées à ceux qui ne devraient pas le savoir ;
- utilisées d'une façon inacceptable ou inattendue au-delà de leur contrôle ; ou
- non gardées en sécurité.

A l'échelle de la société, les risques sont :

- l'immixtion excessive dans la vie privée, ce qui est souvent perçu comme inacceptable ;
- la perte d'autonomie ou de dignité ;
- la prise de décision arbitraire concernant les individus ou la stigmatisation ou l'exclusion de ceux-ci ;
- la montée en puissance excessive du pouvoir organisationnel ;
- un climat de peur, de suspicion ou de manque de confiance.

Il y a trois ans de cela, un journal a rendu compte de la mise en garde du commissaire à l'information sur le risque d'une société :

> … dérivant sans en être conscient vers une société de surveillance…[24]

Le fait de s'identifier est une composante essentielle dans la lutte contre les actes criminels et donne droit à des services spécifiques ou d'accès à certains lieux. L'approche du gouvernement du Royaume-Uni, qui met en jeu les cartes d'identité, n'a pas fait l'unanimité en matière de coût, de commodité et de respect de la vie privée. En faisant des observations sur la législation de base, le Commissaire à l'information a manifesté ses préoccupations sur la façon dont ces mesures se sont développées, avec notamment la création d'un Registre national d'identité.[25]

La loi de 2006 relative aux cartes d'identité (Identity Cards Act 2006) a été adoptée. Nos inquiétudes concernant certains points fondamentaux des propositions du gouvernement ont attiré l'attention des parlementaires qui les ont reprises lors de l'adoption de la législation. Nous avons exprimé nos inquiétudes de longue date, à savoir que les propositions représentaient beaucoup plus qu'une simple carte d'identité, et manifesté des préoccupations plus grandes concernant la création d'un Registre national d'identité.

Si des changements limités mais bienvenus ont été effectués lors de l'adoption de la législation, nous sommes toujours préoccupés par l'importance des données recueillies et détenues par le gouvernement et à leur usage éventuel dans la pratique. Cela est particulièrement vrai pour la « trace des données » enregistrée lorsqu'une carte est vérifiée, car elle peut permettre de brosser un tableau détaillé sur la façon dont les individus vivent leur vie.

---

[23] GREAT BRITAIN. Information Commissioner. Evidence Submitted by the Information Commissioner to the House of Lords Select Committee on the Constitution Inquiry into 'The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State' Wilmslow, Information Commissioner's Office, 2007

[24] Beware rise of Big Brother state, warns data watchdog. *The Times*. 16 August 2004.

[25] GREAT BRITAIN. Information Commissioner. *Identity Cards Web Page.* (Accessed: April 2008.) http://www.ico.gov.uk/Home/about_us/news_and_views/current_topics/identity_cards.aspx

Les inquiétudes sont parfois exprimées non seulement sur la nature et l'importance des informations recueillies, mais aussi sur la façon dont elles peuvent être regroupées et utilisées. Là encore, il existe une vrai tension entre la protection de la vie privée et l'exploitation de l'usage optimale des systèmes et des ressources financé avec l'argent des contribuables. Dans une approche trop centralisée du partage des données, les dangers perçus sont mis en balance avec la tentative de mener à bien une action suivie face à l'administration gouvernementale et d'éviter ce qui est décrit comme une façon de penser et de travailler « en vase clos ». On parle encore « d'aboutir à un gouvernement intégré ». Aux Etats-Unis, le concept de centres de fusion des données dans lesquels les données peuvent être regroupées et analysées pour lutter contre le crime est répandu. Il a été énoncé dans un livre de recommandations[26] publié par le Ministère de la justice comme :

> … un mécanisme effectif et efficace pour échanger des informations et renseignements, maximiser les ressources, réduire les opérations et améliorer la capacité de lutte contre le crime et le terrorisme par l'analyse de données de sources diverses.

Rassurantes d'une certaine manière, les recommandations sur la gestion des centres de fusion soulignent la nécessité de garantir la protection des droits constitutionnels, des libertés civiles, des droits civils et de la vie privée dans le processus de renseignement.

L'individu et les services de bibliothèque et de l'information

Les services de gestion axés sur les personnes et l'information placent ostensiblement les obligations éthique et légale en matière de données à caractère personnel au-dessus des gestionnaires des services de bibliothèque et de l'information. Dans la conduite de leurs activités, ces derniers utilisent les données à caractère personnel dans des tâches et applications diverses. Les activités portent entre autres sur des interactions avec un ensemble de personnes, notamment : les membres du corps dirigeant ou des organismes de financement, les fournisseurs d'équipements et de matériels, les employés, les partisans et enfin, et non les moindres, leurs portefeuilles clients composés d'usagers ou d'usagers potentiels. Les applications générales mettant en jeu des données à caractère personnel sont :

- les éléments d'information sur les utilisateurs en qualité de membres et leurs (éventuels) intérêts
- les questions substantielles/registres du prêt
- les historiques des services fournis ou à fournir aux utilisateurs
- les dossiers d'information spécialisés sur des personnes et des organisations (par exemple, les associations locales, les Amis de bibliothèque)
- les dossiers sur le personnel, notamment des fichiers de paie
- les comptes/factures et registres de commande
- le courrier électronique
- les données à caractère personnel peuvent également subsister dans des bases de données et catalogues de documents (par exemple les catalogues interrogeables en ligne assortis de noms d'auteurs personnels) et les pages Web.

Des efforts visant à promouvoir des services particuliers, à cibler des groupes précis ou à accroître le champ ou l'importance des services proposés peuvent porter sur le recueil et l'analyse des données plus spécifiques concernant les individus dans le domaine du service. L'établissement du profil d'une

[26] UNITED STATES. Department of Justice. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.* Washintgton, US DoJ, 2006.
http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf

population contribue à orienter les services et les ressources à des groupes présentant des besoins et des intérêts particuliers. Parmi les exemples tirés des bibliothèques publiques, on peut citer : les informations aux personnes présentant des déficiences visuelles, les personnes âgées et les enfants, ou celles intéressées par l'histoire de la famille. Il est possible de trouver dans les bibliothèques d'établissements d'enseignement supérieur des exemples de données notamment sur les besoins particuliers des personnes qui suivent des cours à distance ou des personnes souffrant de dyslexie ou de déficience visuelle. De plus, les algorithmes appliqués aux données sur les emprunts de livres permettent de rassembler et présenter des recommandations de « lecture conseillée » tirées des tendances d'emprunt des utilisateurs de la même manière que l'approche axée sur le client d'Amazon. Tous ces efforts visent manifestement à offrir des services ciblés et de meilleure qualité, mais ils entraînent l'acquisition de données à caractère personnel supplémentaires, parfois sensibles, qui peut être perçue par certains comme un acte intrusif et qui porte atteinte à l'intimité de la vie privée. Cependant, une étude réalisée au Royaume-Uni et publiée en 2002 a montré que les usagers des bibliothèques étaient généralement très peu soucieux des questions touchant leur vie privée. Par ailleurs, ces derniers ont de grandes attentes et manifestent un niveau raisonnable de confiance sur la façon dont les services de bibliothèque et de l'information gèrent les données à caractère personnel les concernant. L'étude a également montré que les gestionnaires pourraient bénéficier de lignes directrices sur la politique à suivre et de pratiques d'excellence dans ce domaine.[27]

Un empiétement plus grave sur la vie privée concerne les exigences et les dilemmes auxquels les gestionnaires peuvent parfois être confrontés lorsqu'ils reçoivent des demandes des autorités responsables de l'application de la loi de communiquer des détails concernant l'usage d'informations et les habitudes d'emprunt d'un individu pour les aider à détecter les actes criminels ou le terrorisme. Les questions éthiques et celles liées à la profession en matière de confidentialité entrent en conflit avec des aspects sociaux et des obligations légales dans une perspective plus large. En général, les gestionnaires conservent ces informations jalousement pour ne pas trahir la confiance des usagers et opèrent seulement sur directives des tribunaux ou sur ordre judiciaire.

Aux Etats-Unis, les gestionnaires des services de bibliothèque et de l'information et le public sont particulièrement préoccupés par le nombre de visites et d'interrogations des agents de l'application de la loi, notamment des agents du FBI, et ce plus particulièrement après les événements du 11 septembre 2001 et l'adoption par la suite de la *Patriot Act*,[28] ainsi que l'utilisation des Lettres concernant la sécurité nationale (*National Security Letters*) pour étayer leurs investigations. La profession a réagit de manière positive pour protéger la vie privée en instaurant un système d'équilibre judicieux entre pouvoirs et contre-pouvoirs. L'Association des bibliothèques américaines[29] (*American Library Association*) a fourni une assistance et des conseils importants dans ce domaine.

Les attraits séduisants cet expédient à court terme menacent de ternir un principe plus profond au travers duquel la société se protège et par lequel il est jugé. Benjamin Franklin le dit très succinctement :

> Ceux qui sont disposés à renoncer à une liberté fondamentale pour acquérir un peu de sécurité temporaire ne méritent ni liberté ni sécurité.

[27] Sturges, P., Davies, J.E., Dearnley, J., Iliffe, U and Oppenheim, C. *Privacy in the Digital Library Environment*. London, Resource, 2002. (Library and Information Commission Research Report 135).
[28] UNITED STATES. Laws, Statutes. USA Patriot Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. 2001
[29] AMERICAN LIBRARY ASSOCIATION. *Confidentiality and Coping with Law Enforcement Inquiries: Guidelines for the Library and its Staff Web Page*. (Accessed: April 2008)
http://www.ala.org/ala/oif/ifissues/confidentiality.cfm

Recommandations et déontologie

Dans l'agitation et l'incertitude de la gestion quotidienne, il convient de réfléchir sur la façon dont les gestionnaires de services de bibliothèque et de l'information, parfois confrontés à des priorités et exigences contradictoires, se prononcent sur le comportement le plus éthique à adopter. En plus des obligations de la loi et la conscience propre, les principes, les lignes directrices et les codes éthiques mis à disposition par diverses organisations professionnelles à l'heure actuelle aident à déterminer les frontières du comportement éthique et professionnel. Ils servent de points de référence par rapport auxquels les décisions peuvent être évaluées et jugées par la suite. Ces exemples existent en grand nombre de part le monde et le site de l'IFLA propose une longue liste avec des liens utiles.

Les quatre exemples choisis ici en guise d'illustration sont sans équivoques quant à l'importance de la vie privée, comme le démontreront ces extraits.

- L'Institut officiel des professionnels des bibliothèques et de l'information (CILIP, *Chartered Institute of Library and Information Professionals*) [Royaume-Uni][30]

Douze principes éthiques pour les professionnels de bibliothèque et de l'information qui caractérisent leur conduite sont énumérés. Deux d'entre eux sont particulièrement pertinents :

> Intérêt pour le bien public pour toutes les questions liées à l'exercice de la profession, notamment le respect de la diversité au sein de la société, et la promotion de l'égalité des chances et des droits de l'homme.
>
> Respect de la confidentialité et de la vie privée vis à vis des usagers de l'information

De plus, le Code de la pratique professionnelle des professionnels de bibliothèque et de l'information prescrit des comportements professionnels classés en cinq catégories :

A. Responsabilités personnelles
B. Responsabilités vis à vis de l'information et ses usagers
C. Responsabilités vis à vis des collègues et des acteurs de l'information
D. Responsabilités vis à vis de la société
E. Responsabilités en tant qu'employés

Ces catégories sont étayées par des études de cas, ce qui renforce l'interprétation.

La vie privée et la confidentialité sont abordées dans les catégories :

> B. Responsabilités vis à vis de l'information et ses usagers
>
> 4. Protéger la confidentialité pour toutes les questions relatives aux usagers de l'information, notamment leurs interrogations, les services à fournir quels qu'ils soient, et tous les aspects de la situation personnelle de ces usagers ou de leurs affaires privées.

et

> D. Responsabilités vis à vis de la société
>
> 3. S'efforcer de trouver un juste équilibre dans un cadre légal entre les exigences des usagers de l'information, la nécessité de respecter la confidentialité, les termes de l'utilisation de l'information, le bien public et les responsabilités exposées dans ce Code.

[30] CHARTERED INSTITUTE of LIBRARY and INFORMATION PROFESSIONALS. CILIP Professional Ethics Web Page. (Accessed: April 2008)
http://www.cilip.org.uk/policyadvocacy/ethics

- Association des bibliothèques américaines (ALA, *American Library Association*) [Etats-Unis][31]

Le Code de déontologie de l'ALA, adopté en 1997 et amendé en 2008 comprend huit déclarations sur le comportement professionnel et comporte la déclaration suivante relative aux données à caractère personnel et à la vie privée :

> Nous protégeons le droit de chaque usager de bibliothèque à l'intimité de la vie privée et à la confidentialité concernant les informations recherchées et reçues et les ressources consultées, empruntées, acquises ou transmises.

En outre, l'ALA s'est montrée très active dans l'élaboration des politiques et des conseils relatifs au *Patriot Act* mentionné plus tôt.

- Association australienne des bibliothèques et de l'information[32] (ALIA, *Australian Library and Information Association*)

La déclaration de l'ALIA sur la conduite professionnelle précise le principe sous-jacent gouvernant la conduite ainsi qu'une observation générale sur les normes et les responsabilités qui doivent être respectées. Elles sont présentées plus en détail en cinq déclarations d'action séparées.

> Principe : les personnes engagées dans les services de bibliothèque et de l'information sont membres d'une profession attachée au respect de la liberté intellectuelle et à la libre circulation des idées et de l'information.
>
> Observation : Parce que les services de bibliothèque et de l'information ont pour rôle de favoriser le bien-être social, culturel et économique de leurs publics, les personnes qui travaillent dans ces services ont des responsabilités dans le recueil, l'organisation et la fourniture d'accès à l'information aux clients de leurs services. Les interactions entre les services de bibliothèque et de l'information et leurs clients doivent être régies par les meilleures normes en matière de qualité de service et déterminées par les degrés d'intégrité les plus élevés.

Les quatrième et neuvième observations sont importantes pour les questions de vie privée.

> protéger les droits de leurs clients à l'intimité de la vie privée et à la confidentialité
>
> et
>
> traiter les clients et les collègues avec respect.

- Association canadienne des bibliothèques[33] (*Canadian Library Association*)

[31] AMERICAN LIBRARY ASSOCIATION. *ALA Code of Ethics Web Page.* (Accessed: April 2008) http://www.ala.org/ala/oif/statementspols/codeofethics/codeethics.cfm

[32] AUSTRALIAN LIBRARY and INFORMATION ASSOCIATI ON. *ALIA Statement on ProfessionalConduct Web Page.* (Accessed: April 2008) http://www.alia.org.au/policies/professional.conduct.html

[33] CANADIAN LIBRARY ASSOCIATION. *CLA Position Statements Web Page.* (Accessed: April 2008) http://www.cla.ca/AM/Template.cfm?Section=Position_Statements&Template=/CM/HTMLDisplay.cfm&ContentID=4912

Le Code de déontologie de l'Association canadienne des bibliothèques, adopté en 1976, est extrêmement bref avec ses quatre clauses qui décrivent succinctement la responsabilité individuelle et collective requise pour en être membre. La toute dernière traite des questions de la vie privée.

> Les membres… ont la responsabilité individuelle et collective de :
> protéger la vie privée et la dignité des usagers et du personnel des bibliothèques.

De plus, sa *Déclaration sur l'accès des citoyens aux banques de données – Le droit à la vie privée*, comporte également la politique suivante :

> Que les noms des usagers de bibliothèque ne soient pas délivrés à une personne, une institution une association ou une agence quel qu'en soit les raisons, sauf dans le cas où ceux-ci sont légalement requis par des lois fédéraux ou provinciaux.

Conclusion

Les services de bibliothèque et d'information fournissent depuis longtemps l'accès à l'information pour tous, sans entrave ou qualification, en tenant compte des droits de l'individu à la liberté et à la sécurité. Il convient aux professionnels de s'impliquer dans des discussions concernant l'utilisation et la protection des informations à caractère personnel de part le monde. Cela implique le respect de la vie privée des individus et l'attention accordée à la fiabilité et à l'utilisation adéquate des informations sur les personnes. Les gestionnaires des bibliothèques et de l'information, du fait de leurs parcours et expertise en matière de recueil, d'organisation et d'exploitation des données, ainsi que leurs ethos professionnels dans le service et leur équité, sont bien placés pour contribuer au développement des politiques et pratiques qui garantissent, aujourd'hui comme demain, un traitement approprié des données à caractère personnel.