UN HISTORIQUE DE LA NORMALISATION DANS LE DOMAINE DE PROTECTION DE LA VIE PRIVÉE : DOCUMENT D'INFORMATION

Préparé pour

l'Atelier sur la normalisation en matière de protection de la vie privée

Conseil canadien des normes

22 février 2007

par
Colin J. Bennett, Ph.D.
Professeur au Département de science politique,
Université de Victoria
Robin Bayley, Directeur principal,
Linden Consulting, Inc.
Victoria, Colombie-Britannique

14 février 2007

cjb@uvic.ca
http://web.uvic.ca/poli/bennett

cjb@uvic.ca
http://web.uvic.ca/poli/bennett

TABLE DES MATIÈRES

PAGE

I. INTRODUCTION

Le présent document d'information a pour objet :

- de fournir une justification en faveur des normes de management de la protection de la vie privée ;
- de tracer l'histoire de ces tentatives, d'abord au sein de l'Association canadienne de normalisation (CSA) et, subséquemment, à travers l'Organisation internationale de normalisation (ISO) et le Système de normalisation de la société de l'information élaboré par le Comité européen de normalisation (CEN/ISSS); et
- de tenter, en conclusion, de comprendre les raisons pour lesquelles une activité aussi intense a donné à ce jour des résultats bien modestes.

Ce document servira de contexte descriptif dans l'attente d'un document plus ample et analytique qui doit être rédigé en prévision de la Conférence annuelle internationale des Commissaires à la protection des données personnelles et de la vie privée qui se tiendra à Montréal, en septembre 2007.

II. JUSTIFICATION DES NORMES DE MANAGEMENT DANS LE DOMAINE DE LA PROTECTION DE LA VIE PRIVÉE

Dans les années 1970 et 1980, on présumait communément que le seul instrument nécessaire pour la protection des renseignements personnels était une loi régissant la confidentialité des renseignements (protection des données) encadrée par une autorité de contrôle indépendante (agence de protection des donnés ou de la vie privée). Dans les années 1990, ces suppositions ont évolué. Il était assurément nécessaire de légiférer en la matière, mais cette mesure n'était pas une condition suffisante pour la résolution de la myriade des problèmes rencontrés pour la protection des renseignements personnels dans un environnement connecté et maillé en réseaux. D'autres instruments d'autoréglementation et issus de la technologie devaient contribuer à leur solution. C'est dans ce contexte qu'est née l'idée d'une norme consacrée à la protection des renseignements personnels[1].

À la différence de la majorité des normes qui se rapportent à la fabrication de produits et dont la nature est essentiellement technique, les normes de management donnent des garanties afférentes à un processus, non à un produit. Dans les années 1990, l'impulsion pour l'élaboration d'une norme de management en matière de protection de la vie privée est issue des facteurs suivants :

[1] Voir Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press, 2006).

1) La reconnaissance du fait que la mise en œuvre efficace d'une politique de protection de la vie privée concerne dans une large mesure les processus organisationnels : par ex., l'assurance de procédures appropriées de résolution de plaintes ; la détermination du niveau et du type de collecte de données personnelles ; l'application de mesures de protection adéquates ; la transparence des politiques et des pratiques, et ainsi de suite.
2) Les similarités observées entre les exigences d'une politique de protection de la vie privée et d'autres normes de management de la qualité (par ex., ISO 9001) et la reconnaissance du fait que la protection de la vie privée pouvait être intégrée à cet environnement d'établissement des normes et de certification.
3) L'expansion, l'intégration et la prolifération du commerce électronique mondial et le besoin de dissiper les inquiétudes des consommateurs sur la confidentialité et la sécurité des renseignements à caractère personnel.
4) Sur l'Internet, la reconnaissance que les organisations pouvaient obtenir des titres de compétences en matière de protection de la vie privée à travers une gamme de programmes de sceaux de confidentialité sans une mise en œuvre intégrale de bonnes pratiques.
5) L'externalisation par le gouvernement du traitement de données personnelles créant de situations dans lesquelles les entrepreneurs n'étaient pas tenus aux mêmes normes de protection de la vie privée que les organismes gouvernementaux.
6) L'absence de pouvoirs d'audit adéquats et de ressources suffisantes à l'intérieur des divers organismes de protection des données et des renseignements personnels[2].
7) Le problème de déterminer la comparabilité des normes sur la protection de la vie privée sur le plan international et la difficulté de savoir si de tels instruments étaient mis en œuvre adéquatement (c.-a-d. en vertu du test d'« adéquation » dans le cadre de la Directive européenne en matière de protection de données)[3].

Les opinions diffèrent sur la structure qu'il convient de mettre en place pour la protection de la vie privée. Un consensus semble se dessiner autour de ces caractéristiques :

- une traduction des principes d'équité adoptés[4] pour le traitement des données personnels dans le langage et le format des normes ;

[2] David H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989).
[3] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[4] La codification de ces principes varie. Ils peuvent être ramenés essentiellement à ces pratiques. Une organisation (publique ou privée) :
- est *responsable* de tous les renseignements personnels en sa possession,
- doit *déterminer les finalités* pour lesquelles les renseignements sont traités, et ce préalablement ou au moment de la collecte,

- des directives distinctes sur l'application de ces principes dans les organisations;
- des outils d'évaluation de la conformité appropriés à la taille de l'organisation et au degré de sensibilité des données personnelles traitées;
- un guide d'audit;
- un système pour l'accréditation d'auditeurs chargés du respect de la vie privée.

III. HISTORIQUE DE LA NORMALISATION EN MATIÈRE DE MANAGEMENT DE LA PROTECTION DE LA VIE PRIVÉE

Trois organismes de normalisation principaux se sont employés au cours de la dernière décennie à tenter d'élaborer une telle norme dans le domaine de la protection des renseignements personnels : l'Association canadienne de normalisation (CSA), l'Organisation internationale de normalisation (ISO) et le Comité européen de normalisation et son Système de normalisation de la société de l'information (CEN/ISSS).

Le Code type sur la protection des renseignements personnels de la CSA

Les travaux en vue de l'élaboration d'un « code de protection des renseignements personnels » ont débuté au sein d'un comité technique de la CSA en 1993. Les négociations se sont prolongées pendant un certain temps, mais le 20 septembre 1995 était adopté le *Code type sur la protection des renseignements personnels* (Code type). Le Code fut subséquemment approuvé à titre de norme nationale du Canada (Q830) par le Conseil canadien des normes en mars 1996.

Le Code type de la CSA s'articule autour de dix principes accompagnés de leur commentaire interprétatif respectif. Il était préconisé que les organisations et les associations commerciales intègrent en totalité ces principes dans leurs codes de pratiques et les appliquent aux conditions sectorielles particulières. Le Code

---

- doit recueillir des renseignements personnels seulement avec la *connaissance et le consentement* de la personne (sauf dans des circonstances définies),
- doit *limiter la collecte* des renseignements personnels aux éléments nécessaires à la poursuite de fins déterminées,
- ne doit utiliser ou divulguer des renseignements personnels à des fins autres que celles pour lesquelles ils ont été déterminés, à moins que la personne n'y consente (*principe de finalité*),
- ne doit *conserver* l'information que pour le temps nécessaire.
- doit s'assurer que les renseignements personnels sont *exacts, complets et à jour,*
- doit protéger les renseignements personnels au moyen de *mesures de protection* adéquates,
- doit être *ouverte* au sujet de ses politiques et pratiques et ne garder aucun système d'information secret,
- doit permettre à la personne *l'accès* aux renseignements personnels la concernant, en lui donnant la possibilité de les modifier s'ils se révèlent inexacts, incomplets ou obsolètes.

type appuyé d'un atelier donnant un plus grand nombre de conseils pratiques et d'interprétations. Dans le même temps, d'aucuns envisageaient l'étendue du Code type à tous les secteurs de l'économie canadienne par effet des pressions du marché, de la persuasion morale, des obligations contractuelles et d'un sentiment général au sein de l'entreprise que celle-ci était la voie obligée pour éviter la réglementation gouvernementale.

Bien que le Code type emploie certains termes normatifs tels que « doit » ou « s'impose », il a été conçu comme un instrument volontaire dans le sens où il n'était aucunement contraignant à l'égard des organisations. Une fois adopté, cependant par une organisation, le Code type visait à produire les mêmes effets que toute autre norme. Les allégations se réclamant du code entraînerait des obligations : les organisations seraient tenues de *dire ce qu'elles font* et de *faire ce qu'elles disent*. En conséquence, en 1996, le Quality Management Institute (QMI) annonçait un programme de reconnaissance créé pour permettre aux entreprises d'adhérer au Code type et de démontrer ainsi leur conformité. Ce programme de reconnaissance était sensible au fait que les obligations en matière de respect de la vie privée d'une grande banque, d'une compagnie d'assurances et d'une firme de vente directe différaient de celles d'une PME ou d'une entreprise locale[5]. Ainsi, à la différence d'autres instruments d'autoréglementation telles que les lignes directrices de l'OCDE[6], le QMI précisait clairement ce que l'« adoption » du Code type signifiait. Les entreprises seraient tenues d'élaborer un code de pratiques cohérent, de produire un ensemble de lignes directrices pour sa mise en œuvre interne et de présenter ensuite une demande de certification auprès d'un organisme d'enregistrement accrédité. À l'instar d'autres normes, le Code type de la CSA se devait d'être enregistré et visait à motiver une certaine continuité sur le marché et un niveau plus élevé de confiance chez les consommateurs.

L'application de ce Code type n'a jamais été mise entièrement à l'essai à cause de la décision, prise par le gouvernement canadien en 1999, de légiférer en la matière et d'y astreindre le secteur privé. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ) a commencé à produire ses effets en 2001. Son dessein central était d'exiger des organisations engagées dans une activité commerciale au Canada de se conformer au Code type, reproduit textuellement à l'Annexe 1 de la loi. Celle qui avait commencé comme une mesure innovatrice d'autoréglementation était dépassée sous l'impulsion de pressions politiques et législatives.

En promulguant la LPRPDÉ , le législateur était déterminé à s'inspirer du Code type de la CSA pour une raison bien précise. On croyait tout d'abord que, puisque le secteur privé avait déjà négocié cette norme, la mesure de loi n'aurait d'autre effet que d'obliger les entreprises à « s'en tenir aux règles qu'elles

[5] CSA, PLUS 8830 – *Implementing Privacy Codes of Practice*, Colin J. Bennett, août 1995.
[6] Organisation de coopération et développement économiques (1981), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personne*, (Paris : OCDE).

s'étaient elles-mêmes fixé ». Deuxièmement, et ce point s'est perdu, le Code type de la CSA est en soi un mécanisme de levier crucial susceptible d'augmenter les ressources modestes du Commissariat à la protection de la vie privée du Canada afin de garantir un bon niveau de conformité. Une fois qu'une organisation est enregistrée, le Code type cesse d'être un mécanisme « volontaire ». Cette organisation devra se doter d'un code et d'un ensemble connexe de lignes directrices opérationnelles et être assujettie à un *processus de vérification périodique et indépendant* de ses pratiques de la part d'un organisme d'enregistrement accrédité. La sanction, à la suite d'une plainte bien fondée, est non seulement une amende mais l'obligation de modifier ses pratiques à l'issue de la vérification. Inversement, la démonstration qu'un code de pratiques est véritablement appliqué dans toute l'organisation devrait avoir une rare puissance probante. Cela ne devrait pas exempter des dispositions de la LPRPDÉ, mais devrait ajouter du poids à toute investigation ou procédure devant le Commissaire ou les tribunaux.

Qui plus est, l'enregistrement du Code type de la CSA aiderait à l'interprétation et à l'observation du principe 4.1.3 qui exige de la part des organisations de « fournir, par voie contractuelle ou autre, un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie ». Il pourrait également aider à répondre à la délicate question de savoir comment assurer des niveaux comparables de protection quand le traitement des données personnelles est imparti par une entreprise canadienne à une organisation outre-mer. Les contrats pourraient alors faire référence à la norme dont l'enregistrement est une condition pour le traitement continu de données personnelles canadiennes.

Le besoin d'une certification a-t-il été rendu redondant par l'inclusion du code dans la LPRPDÉ? Pourquoi les organisations prendraient-elles la peine de consacrer du temps et de l'argent pour être en mesure de démontrer leur conformité par la voie d'une certification, dès lors qu'elles sont déjà tenues au respect de ces règles par la loi ?

D'après le rapport annuel 2005 de la Commissaire sur la LPRPDÉ, « il convient de noter que, des 401 plaintes déposées, seules 77 % d'entre elles (19 %) ont été jugée non fondées », une indication que les organisations ne se conforment pas massivement aux dispositions de la loi. Un grand nombre d'entre elles connaissent mal ses exigences et des personnes sont lésées par des pratiques non conformes[7]. Il semblerait que, dans la mesure où elles connaissent la loi, beaucoup d'organisations se contentent d'attendre qu'une plainte soit formulée, sachant qu'elles pourront démontrer de bonnes dispositions durant les investigations et les médiations et éviter ainsi d'être pénalisées. D'autres entreprises estimeront, inconsciemment peut-être, qu'elles ne prennent pas de risques commerciaux et remettent à plus tard tout changement de leurs pratiques

[7] Voir par ex., John Lawford, *Consumer Privacy under PIPEDA: How are we Doing?* (Centre pour la défense de l'intérêt public : novembre 2004).

de renseignements personnels au lieu d'attendre de savoir les points sur lesquels les personnes ont des objections. Il semble bien qu'en acquérant force de loi, de proactive qu'elle était, la norme de la CSA soit devenue un instrument plus réactif.

La tentative d'élever le Code type au rang de Norme internationale par l'entremise de l'ISO

Dès la fin des années 1990, les observateurs manifestaient le désir de voir internationalisée la norme nationale du Canada et des pressions ont été exercées sur l'ISO pour que l'organisation reprenne le flambeau. Les lois en faveur de la protection de la vie privée se multipliaient dans le monde et les réglementations se damaient le pion car les pays et les régions essayaient de s'arroger des avantages concurrentiels dans le domaine du commerce électronique. Les entreprises recherchaient également des moyens de simplifier et d'améliorer la confiance dans leurs pratiques de sous-traitance et d'impartition de processus connexes au traitement des renseignements personnels.

Beaucoup estimaient qu'une norme distincte de l'ISO en matière de protection de la vie privée desservirait les intérêts de toutes les nations et de tous les intervenants. Elle aurait un bien plus grand poids et une crédibilité accrue dans le monde en bénéficiant ainsi à un plus grand nombre de personnes et d'organisations. Elle attirerait de l'attention et des efforts de certification à l'échelle internationale de la part des différents organismes nationaux de normalisation. Et elle donnerait à des entreprises opérant dans des pays jugés non adéquats en vertu du droit européen de protection des données une méthode plus fiable et cohérente grâce à laquelle elles pourraient démontrer leur conformité aux normes de protection des données internationales[8].

En mai 1994, le comité des associations de consommateurs de l'ISO (COPOLCO) a constitué un groupe de travail pour déterminer si ce qui était alors un projet de norme de l'Association canadienne de normalisation pouvait être le fondement d'une norme internationale pour la protection des renseignements personnels. Le groupe recommanda au COPOLCO en avril 1996 l'élaboration par l'ISO d'une norme internationale. Le Conseil de l'ISO a accepté cette recommandation en septembre 1996 et décidé que les avancées rapides de la technologie et l'expansion de la communication électronique et des bases de données exigeaient des règles mondiales pour la protection des renseignements personnels. Il fit remarquer que, bien que les réglementations diffèrent dans le monde, des normes consensuelles pouvaient contribuer à assurer une base de protection globale. Le Conseil de l'ISO a demandé également au secrétaire général de transmettre la recommandation du COPOLCO au Bureau de gestion

[8] Voir l'argumentaire dans : Colin J. Bennett, *Prospects for an International Standard for the Protection of Personal Information: A Report to the Standards Council of Canada* (August 1997) at: http://web.uvic.ca/~polisci/bennett/research/iso.htm

technique (TMB) pour des mesures appropriées, conjointement avec les commentaires formulés durant la réunion.

En déterminant comment les travaux seront entamés dans le cadre de la normalisation pouvait débuter, les douze membres du TMB de l'ISO ont décidé de saisir de la question un groupe consultatif spécial ad hoc (AHAG) en janvier 1997. L'AHAG était censé produire un avis de résolution positive du TMB en 1998. Toutefois, les réserves émises au sujet de cette initiative de la part des représentants de l'American National Standards Institute (ANSI) avaient déjà circulé et la résolution attendue ne s'est pas matérialisée. L'AHAG a poursuivi l'étude de la question pendant une autre année mais il a été dissous en juin 1999. Une réunion qui s'est tenue à Hong Kong plus tard dans la même année parvint à la conclusion que d'autres instruments de normalisation utiles à peine moins articulés qu'une norme au plein sens du terme pouvaient être négociés, mais que le projet d'une norme de management générale devait être mis « en veilleuse ». Le groupe reconnaissait que les travaux seraient repris par le Comité européen de normalisation (CEN) et était disposé à réexaminer la question, sur demande.

Des travaux connexes ont été poursuivis indépendamment par un comité technique mixte de l'ISO et de la Commission électrotechnique internationale (JTC-1). Ce comité mixte a élaboré plusieurs normes de base dans le domaine des technologies de l'information et de la communication dont certaines contenaient des composantes clés de protection de la vie privée[9]. Des sous-comités du JTC-1 avaient abordé ces questions : cartes d'identité et identification personnelle ; techniques de sécurité de la TI ; identification automatique et techniques de saisie de données (RFID); gestion et échange de données ; technologie de l'information pour l'apprentissage, l'éducation et la formation ; et biométrie.

Un autre organisme important est l'International Security, Trust and Privacy Alliance[10] qui avait travaillé indépendamment à une norme-cadre sur la protection de la vie privée en 2003. L'ISTPA avait élaboré ce cadre, conçu comme « une aide complète et précieuse pour ceux qui appliquent des politiques de protection de la vie privée dans des systèmes d'information contenant des renseignements identifiables à caractère personnel »[11]. Le projet a été soumis

[9] Publications de 2006 dans le domaine de la protection de la vie privée : Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems and Multimedia security - Guideline for privacy protection of equipment and systems in and out of use, with work in progress on Multimedia Security - Guideline for privacy protection of equipment and systems in use and disused - Part 2: Software method for privacy protection (TC 100). Voir http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=seabox1.p&seabox1=privacy.

[10] L'ISTPA est une coalition mondiale d'entreprises, institutions et fournisseurs de technologie œuvrant de concert pour éclairer et résoudre des questions actuelles et évolutives relatives à la sécurité, à la confidentialité et à la protection des renseignements personnels. Pour en savoir plus sur l'ISTPA et son action, consulter http://www.istpa.org/.

[11] Borking, John J., Privacy Standards for Trust, October, 2005, p. 5 à l'adresse : http://www.privacyconference2005.org/fileadmin/PDF/borking.pdf

subséquemment par l'International System Security Engineering Association (ISSEA) à titre de Spécification publiquement disponible (PAS) de l'ISO[12] et porté à l'attention des commissaires à la protection des données et à la vie privée, lors de la Conférence internationale tenue à Wroclaw, Pologne, en 2004.

Les commissaires à la protection des données n'ont pas été par le passé très engagés dans des activités liées aux normes. Toutefois, leur Groupe de travail Art. 29 a émis une opinion le 29 mai 1997 et exprimé son soutien en considérant que « de telles initiatives contribuent d'une manière significative à la protection des droits fondamentaux et de la vie privée à l'échelle mondiale »[13]. À Wroclaw, les commissaires ont adopté une résolution recommandant « qu'une norme internationale de protection de la vie privée et particulièrement une norme concernant les technologies de protection de la vie privée soit élaborée par l'ISO, pour favoriser la mise en œuvre des obligations légales en matière de protection des données et de la vie privée là où elles existent et la formulation de ces obligations là où elles font défaut ». Ce faisant, les commissaires exprimaient également leur préoccupation jugeant que les initiatives de l'ISTPA et du JTC1 étaient en voie de produire des cadres de management incompatibles avec le droit de protection des données européen. Dans une autre résolution, la Conférence décidait que « l'élaboration d'une norme internationale doit être fondée sur les pratiques équitables de traitement des renseignements ainsi que sur les principes de rareté, minimisation et anonymisation des données »[14].

Les travaux du CEN/ISSS

Le Comité européen de normalisation (CEN) a été fondé en 1961 par les organismes nationaux de normalisation au sein de la Communauté économique européenne et les pays de la zone de libre échange européenne[15]. Aujourd'hui, le CEN « contribue aux objectifs de l'Union européenne et de l'espace économique européen avec des normes techniques volontaires qui font la promotion du libre marché, la sécurité des employés et des consommateurs, l'interopérabilité des réseaux, la protection environnementale, l'exploitation des programmes de recherche et développement et l'approvisionnement public ».

---

[12] PAS : « Document normatif représentant le consensus au sein d'un groupe de travail », donc moins qu'une norme au plein sens du terme.
http://www.iso.org/iso/en/stdsdevelopment/whowhenhow/proc/deliverables/iso_pas.html

[13] http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/1997_fr.htm

[14] Resolution on a Draft ISO Privacy Framework Standard, ISO/IEC JTC1 SC36# N1231, 2006-02-15, accessible par le site http://jtc1sc36.org/doc/N1201-N1250.html
L'organisation (la fondation Wroclaw) mise sur pied par la suite pour traiter des questions de procédure et faciliter leur reconnaissance officielle dans l'élaboration de la norme n'a jamais vraiment décollé.

[15] Extrait du site Web du CEN, http://www.cen.eu/cenorm/aboutus/index.asp Sa hiérarchie et ses relations complexes sont bien illustrées graphiquement dans le document http://www.cen.eu/cenorm/aboutus/structure+/thecensystem/structure1.ppt.

L'engagement du CEN dans le domaine de la protection de la vie privée a commencé à travers un groupe multilatéral dit d'Initiative pour la normalisation de la protection de la vie privée en Europe (IPSE) qui a remis son rapport in 2002[16]. L'IPSE recommandait que le CEN/ISSS : identifie un ensemble de meilleures pratiques européennes volontaires pour la protection des données; élabore un ensemble générique de clauses contractuelles reflétant les exigences de l'Art. 17 de la Directive européenne; dresse un inventaire des pratiques d'audit dans le domaine de la protection des données ; effectue un sondage des programmes de sceau d'approbation Web au fondement de l'examen d'une normalisation plus poussée ; développe une approche cohérente pour l'évaluation de l'impact des évolutions technologiques en cours ; et de réunir et livrer un ensemble ciblé de documents d'éducation et d'orientation sur les questions de la normalisation ayant trait à la protection de la vie privée.

L'IPSE n'a pas, cependant, recommandé une norme de management au niveau européen en alléguant que « il n'existe dans l'immédiat aucune demande manifeste au niveau européen pour une norme de type management sur la protection de la vie privée ». L'IPSE suggérait également que « tout travail au sujet d'une norme de management européenne est en ce moment prématuré et que les intérêts européens individuels en matière de protection de la vie privée ont une voie qu'ils peuvent emprunter pour poursuivre ces objectifs par l'entremise de l'ISO, partant des résolutions du COPOLCO, si tel est leur vœu »[17].

Les travaux du CEN ont continué par une série d'ateliers de son Système de normalisation de la société de l'information (ISSS), y compris l'atelier européen CEN ISSS sur la Protection des données personnelles et de la vie privée (CEN/ISSS/WS/DPP) dont le but est « d'aider les organisations à se conformer à la Directive sur la protection des données et aux lois nationales pertinentes en facilitant l'harmonisation des pratiques, en développant la compréhension et la prévisibilité de pratiques détaillées ou sectorielles, en contribuant à résoudre les questions de conformité techniques des TIC et en encourageant la continuité de l'évaluation et du suivi »[18]. [Trad.]

L'atelier a déjà produit plusieurs rapports en 2005 et 2006, y compris :

- un inventaire des Pratiques d'audit en matière de protection des données;
- une analyse des technologies de protection de la vie privée, des technologies permettant d'accroître le respect de la vie privée, des systèmes de management de la protection de la vie privée et des systèmes de gestion de l'identité, de leurs pilotes respectifs et du besoin de la normalisation ;

[16] Initiative du CEN/ISSS sur la normalisation de la protection de la vie privée en Europe, rapport final, 13 février 2003. Voir http://ec.europa.eu/enterprise/ict/policy/standards/ipse_finalreport.pdf
[17] Ibid, p. 51.
[18] Site Web du CEN, http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/wsdpp.asp

- un contrat d'adhésion pour aider à la conformité aux obligations imposées aux termes de l'art. 17 de la Directive 95/46/CE sur la protection des données (et son guide de mise en œuvre);
- Cadre d'audit de protection des données (Directive européenne 95/46CE) - Partie I : Cadre de base – La protection des données personnelles dans l'UE ;
- Cadre d'audit de protection des données (Directive européenne 95/46CE) - Partie II : Listes de vérification, questionnaires et modèles pour les utilisateurs du cadre – La protection des données personnelles dans l'UE[19].

En outre, les participants à l'atelier ont prospecté d'autres domaines de travail qui doivent encore être développés, avec un accent sur la petite et moyenne entreprise, l'autoévaluation et un dialogue beaucoup plus étroit entre les entreprises et les organismes de réglementation.

Ces domaines de travail sont :

- un ensemble commun européen de meilleures pratiques volontaires pour le management de la protection des données afin d'aider les entreprises et les gestionnaires de données à se conformer à la Directive et, dans la mesure du possible, le cas échéant, aux diverses lois nationales européennes et aux exigences supplémentaires ;
- des outils d'audit dans le domaine de la protection de la vie privée au sein de l'UE : vers une approche pratique des outils d'audit pour les gestionnaires des données, en leur permettant de procéder à une autoévaluation ; et
- un Système volontaire de dialogue axé sur la technologie : s'assurer que les nouveaux produits et services et les nouvelles technologies sont conformes aux lois de protection des données et de la vie privée pertinentes dont la transposition dans tous les états membres de l'UE peut constituer une tâche difficile pour l'industrie. En outre, les organismes de réglementation se trouvent quelque peu dépourvus devant les nouvelles technologies susceptibles de rejoindre le marché dans un avenir proche.

IV. CONCLUSIONS

Au début de 2007, le paysage de la normalisation dans le domaine de la protection de la vie privée se présente ainsi :

1) Une norme nationale de protection de la vie privée au Canada qui a été rendue presque redondante par la promulgation de la LPRPDÉ.

[19] Site Web du CEN, http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/wsdpp.asp Les ententes CWA peuvent être téléchargées depuis le site http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/cwa/dppcwa.asp

2) Une activité notable au sein du JTC-1 vers la négociation de normes techniques de base, dont certaines ont des composantes et des implications clés dans le domaine de la protection de la vie privée.
3) Une masse de travaux considérables au sein du CEN/ISSS sur l'audit dans le domaine de la protection des données, les procédures contractuelles ainsi que les technologies permettant d'accroître le respect de la vie privée. Toutefois, il n'est pas encore clair comment ces travaux s'intègrent aux tâches quotidiennes des commissaires à la protection des renseignements personnels et de la vie privée et moins encore à la conformité des entreprises européennes aux exigences concrètes de la protection des données.

L'idée d'une norme de management générale – une version internationale du Code type de la CSA – paraît avoir été mise en veilleuse. Cela peut s'expliquer par :

- une certaine réticence des organismes de normalisation à s'engager dans un domaine qui appartient, traditionnellement, à la problématique des droits humains ;
- un scepticisme de la part des défenseurs de la protection de la vie privée et des organismes de réglementation quant à l'opportunité d'associer à cet enjeu un autre ensemble d'institutions internationales ;
- la crainte, parmi les défenseurs de la protection de la vie privée et les organismes de réglementation, à l'égard d'une norme de management générale venant saper la loi de protection des renseignements personnels en vigueur ;
- dans certains domaines, une ferme opposition de la part du secteur privé à l'idée d'une norme de management générale ;
- la prolifération de systèmes et de sceaux de certification sur l'Internet, qui ont permis aux entreprises de donner l'illusion d'une conformité aux principes de protection de la vie privée, sans devoir se soumettre à un processus rigoureux d'enregistrement des normes.

On peut donc s'interroger si le temps n'est pas révolu pour une norme de management de la protection de la vie privée. Malgré tout, le travail se poursuit sur d'autres normes de management internationales et l'ISO a déclaré que « le très grand impact des normes ISO 9001 et ISO 14001 sur les pratiques organisationnelles et le commerce a stimulé le développement d'autres normes et référentiels ISO qui adaptent le système générique de management à des secteurs ou aspects spécifiques »[20]. L'ISO a en effet introduit récemment plusieurs normes relatives aux systèmes de management. Par exemple, l'ISO/CEI 17799:2005 est le code international de bonnes pratiques pour le management de la sécurité de l'information.

[20] Extrait du site Web de l'ISO, http://www.iso.org/iso/fr/iso9000-14000/msstandards/index_five.html

En outre, dans les circonstances contemporaines où les violations des données sont monnaie courante, la vision d'un système de normes pleinement fonctionnel pour la protection de la vie privée compatible avec la loi en vigueur demeure valide. Le processus en vue de l'obtention et du maintien de l'enregistrement attestant de la conformité à une norme peut diminuer la pression s'exerçant sur les commissaires à la protection de la vie privée en tant qu'unique autorité de contrôle. Dans un environnement où le traitement des données personnelles s'effectue à l'échelle mondiale, l'examen minutieux des lois et des contrats ne donne pas aux agences de protection des données européennes l'assurance que les règles seront respectées par l'organisme récepteur. L'enregistrement selon une norme obligeant de se soumettre à des audits périodiques et indépendants donnerait une certitude accrue qu'une protection de données « adéquate » est pratiquée par l'organisation réceptrice, quel que soit le lieu où elle est implantée. La certification peut également donner des garanties plus sérieuses aux consommateurs désireux de faire affaire avec des organismes respectueux de la vie privée– « sérieuses » car l'adhésion d'une organisation à de bonnes pratiques de protection des renseignements et de la vie privée aura fait l'objet d'une vérification indépendante et aussi parce que, en tant que produit d'une autorité en matière de normalisation, ses exigences sont rigoureuses et communes.