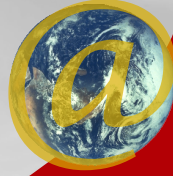
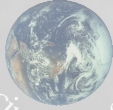


Traitement et protection des données des administrations publiques. Principes et moyens.



COLLOQUE

“Traitement et protection des données  
des administrations publiques.  
Principes et moyens.”



PARLEMENT  
DE LA  
COMMUNAUTÉ FRANÇAISE DE BELGIQUE  
WALLONIE-BRUXELLES



# **Traitement et protection des données des administrations publiques, principes et moyens.**

*Compte rendu du colloque  
organisé par le Parlement de la Communauté française  
le jeudi 20 mars 2008*



# Introduction

*Le colloque commence à 9 h 15.*

## ■ **M. Dechamps, modérateur, Rédacteur en chef de Citizen<sup>e</sup>**

– Le Président ne peut nous rejoindre dans l’immédiat, il nous a demandé de commencer notre colloque. Permettez-moi de commencer par quelques communications techniques. Le débat et les interventions de ce colloque sont diffusés en ligne sur le site du parlement de la Communauté française. Les actes seront publiés d’ici quelques semaines et disponibles au prix de cinq euros. Toutes les informations sont également disponibles sur le site pcf.be ou via la cellule Internet : cellule-internet@pcf.be

La parole est à M. Poulet, Directeur du centre de recherche « Informatique et Droit » des Facultés universitaires Notre-Dame de la Paix de Namur, dont l’introduction s’intitule « La vie privée, un enjeu fondamental pour la démocratie ».



# 1. La vie privée, un enjeu fondamental pour la démocratie

■ **M. Poullet, Professeur aux Facultés Universitaires Notre-Dame de la Paix (FUNDP), Directeur du Centre de Recherches Informatique et Droit (CRID) et du FUNDP**

– Merci Monsieur le Président, permettez moi en exergue de mon propos qui porte précisément sur les liens entre vie privée et démocratie de souligner qu’aujourd’hui, nous vivons un grand moment pour la démocratie, – je ne parle pas simplement du sujet de ce colloque – puisque le gouvernement fédéral est aujourd’hui constitué.

Je commencerai par définir la notion de vie privée et tenterai de montrer combien sa défense constitue un élément fondamental pour la démocratie. Je parcourrai ensuite les développements actuels du gouvernement électronique et ses enjeux pour la sauvegarde de nos libertés. J'aborderai enfin les réponses du droit européen et belge à ces défis et terminerai en lançant un message à la Communauté française : qu’elle prenne résolument ses responsabilités dans ce domaine.

Pour lancer la réflexion sur la vie privée et ses enjeux, j’évoque la décision de principe du tribunal constitutionnel allemand du 15 décembre 1983. Le contenu de cette décision vient d’être réaffirmé voire amplifié dans une décision du 27 février 2008 à propos des limites de la surveillance par les autorités policières des données à caractère personnel générées par notre

utilisation des outils des technologies de l'information et de la communication qui envahissent notre vie quotidienne et dont le trafic laisse des traces à de multiples lieux. « Cette autonomie (la vie privée), affirme, dès 1983, la Cour constitutionnelle, doit être protégée surtout dans les conditions actuelles et à venir du traitement automatisé des données. » Le tribunal énumère ensuite les raisons pour lesquelles il y a péril, comme la puissance et l'intégration des systèmes de traitement qui créent un déséquilibre de forces entre les administrations et les citoyens. Il ajoute: « Si l'individu ne sait pas prévoir avec suffisamment de certitude quelle information le concernant est connue de son milieu social et à qui celle-ci pourrait être communiquée, sa liberté de faire des projets ou de décider sans être soumis à aucune pression est fortement limitée. Si l'individu ne sait pas si un comportement est remarqué et enregistré de façon permanente en tant qu'information, il essaie de ne pas attirer l'attention sur ce comportement. S'il craint que la participation à une assemblée ou à une initiative citoyenne soit officiellement enregistrée, il renonce à l'exercice de ses droits. Ceci n'a pas seulement un impact sur ses chances de se développer, le bien-être commun en est aussi affecté car l'autodétermination est une condition élémentaire fonctionnelle dans une société démocratique libre basée sur la capacité des citoyens d'agir et de coopérer. »

Un mot sur le contexte de cette décision, le tribunal constitutionnel a pris cette décision en 1983 contre la loi « statistique » pourtant votée à l'unanimité par le parlement allemand. L'Etat de droit, c'est-à-dire les principes fondateurs de l'Etat démocratique, lui paraissait devoir l'emporter sur la décision législative. Au-delà le tribunal souligne que les technologies de l'information et de la communication accentuent le déséquilibre entre les pouvoirs informationnels de l'administration et ceux du citoyen. C'est un peu la figure de « Big Brother », selon laquelle l'administration sait tout de nous et peut ainsi décider à notre place.

Une seconde crainte énoncée par la Cour paraît plus subtile. La Cour fait référence au danger que représente l'opacité du fonctionnement des flux et des circuits d'information générée par les technologies de l'information et de la communication. Cette seconde crainte évoque les angoisses dénoncées par un autre roman: *Le Jugement* de Kafka. Dans ce roman, un individu fait l'objet d'un procès dont il ignore la raison et les éléments qui lui sont mis à charge. La question posée ici et là est l'aliénation de la liberté due à l'opacité de l'administration. Cette opacité contient, selon la Cour, le risque d'un conformisme anticipatif, c'est-à-dire le risque de se conformer au comportement que l'on croit être attendu par les personnes qui ont à nous juger.

Le troisième élément est important. La Cour rejette explicitement le point de vue libéral, arguant que la vie privée n'est rien d'autre que la reconnaissance de la propriété par l'individu des informations personnelles à son propos. Au contraire, elle prétend que l'information naît du dialogue entre l'individu et la société et que s'il est donc exclu de parler de propriété, il est essentiel cependant afin de permettre le développement libre de la personnalité que l'individu puisse contrôler et maîtriser cette information. Ce droit à la maîtrise qui suppose non seulement le droit d'accès individuel aux données la concernant mais également le droit à participer à une délibération démocratique qui fixe les principes des traitements, est un droit fondamental et constitue une condition nécessaire à l'ensemble des libertés, celle de s'exprimer qui osera affirmer son opinion s'il ignore ce qui sera fait de son usage de la parole, mais également celle de se loger, de trouver un emploi, de contracter un crédit ou de s'associer.

La vie privée n'est donc pas ce que l'on entend traditionnellement, c'est-à-dire, le droit de se retirer derrière les murs de sa maison, dont on notera qu'ordinateur et autres technologies aidantes ils deviennent de plus en plus pénétrables. La vie privée n'est pas uniquement le droit négatif à la réclusion, à se retirer de la société. De manière plus positive, la vie privée est le droit de participer à la définition de son image et de contrôler son utilisation.

Venons-en aux conséquences que tirera le tribunal constitutionnel de cette importance de la vie privée qu'il estime fondamentale pour l'ensemble des autres libertés. Pour lui, il y a un devoir sacré de l'État de garantir les droits fondamentaux à la liberté de l'individu par des lois sur la protection des données. Suivant l'attendu du tribunal constitutionnel allemand, le standard applicable est le droit de tout un chacun de développer librement sa personnalité. Le droit à l'autodétermination informationnelle est ainsi affirmé.

Si vous voulez permettre à la personne de retrouver une certaine maîtrise de son information, deux mots clés ont leur importance : transparence et proportionnalité des traitements. Ces deux notions renvoient à un débat démocratique. La transparence, synonyme de lutte contre l'opacité, permet à l'individu de savoir dans quels réseaux d'informations circulent ses données personnelles, quelles informations circulent, qui les utilisent et pour quoi faire. Cette transparence est importante et les traitements, de ce fait, doivent être établis par des lois qui en dessinent clairement les contours et répond aux questions rappelées ci-dessus.. Mais cette exigence se double d'une autre : la « proportionnalité » des traitements, qui affirme que les pouvoirs publics comme

les pouvoirs privés ne traitent des données que dans la mesure nécessaire à un besoin d'intérêt général reconnu comme légitime dans une société démocratique. Ainsi il importe que parmi plusieurs voies d'atteindre un objectif on choisisse la voie la moins attentatoire à nos libertés, que l'on s'interroge sur l'importance des justifications amenées à l'appui d'un traitement. S'agit-il de faciliter la vie de l'administration ou au-delà montre t'on qu'il existe un impératif sérieux qui justifie l'atteinte aux libertés. Cette seconde exigence renvoie à la nécessité d'un débat législatif que l'article 22 de la Constitution prône puisqu'il réserve à la loi formelle qu'elle soit fédérale, communautaire ou régionale, le soin de définir les règles d'atteinte à la vie privée. Sans doute, faut-il regretter que dans notre pays, la culture de débats démocratiques en matière de libertés manque. L'installation de la carte d'identité électronique, l'existence d'un numéro d'identification unique pour toutes les administrations n'ont fait l'objet d'aucun débat.

Comment s'est développé « l'e-gouvernement » ? D'une administration en silos, nous sommes passés à une administration en réseau où se multiplient les interconnexions de base de données. Selon mon professeur de droit administratif : Cyr Cambier dont je me plais à rappeler la mémoire,,le droit administratif reposait sur des principes fondamentaux dont celui de la spécialité des administrations. Chacune d'elle, séparée des autres, vit en vase clos. Les échanges entre administrations sont minimes, voire exceptionnels et prévus par une loi spécifique. Ces silos quasiment étanches lui apparaissaient comme la seule garantie possible de nos libertés, permettant d'éviter un trop grand pouvoir de l'Administration, qui concentrerait toute l'information en un point unique.

Sans doute – et que l'on ne s'y méprenne pas, tout est loin d'être négatif au paradis de l'ordinateur- utiliser l'informatique et les TIC permet aujourd'hui à l'administration d'offrir un meilleur service aux citoyens et d'être plus efficace ; l'administration vit de plus en plus en réseau reliant toutes les administrations et s'appuyant sur ce que l'on appelle des sources authentiques de données. Ainsi, le citoyen peut adresser une requête à une administration via un guichet unique commun à plusieurs administrations. Le fait pour l'administration d'être intégrée dans un réseau, éventuellement coordonné par une Banque Carrefour, lui permet d'aller chercher l'information nécessaire à différents endroits. Ainsi, un handicapé qui souhaite obtenir une allocation sociale, qui lui sera accordée en fonction de ses revenus, adressera sa demande à l'Office des personnes handicapées. Celle-ci ira chercher des informations à son sujet dans d'autres administrations de sécurité sociale et, bien sûr, à l'administration fiscale.

L'omniprésence des interconnexions entre administrations peu importe le niveau de pouvoir auquel se rattache l'administration produit plusieurs effets.

Le premier est le besoin d'identifiant. En Belgique, nous avons fait le choix d'un identifiant unique. Toutes les administrations utilisent – même si un identifiant différent a été, jusqu'il y a peu, évoqué pour la santé – le numéro de registre national. La signature électronique liée à la carte d'identité servira de sésame qui ouvrira l'ensemble des portes de cette administration électronique.

Un tel choix confère une grande efficacité aux interconnexions entre administrations.

La lutte contre la fraude fiscale, évoquée dans la déclaration gouvernementale, mérite également notre attention. Dans les administrations se développent le « *datawarehouse* » et le « *datamining* » : les administrations ont de plus en plus la possibilité de glaner des données dans les autres administrations et d'établir des corrélations entre ces données, cela afin de mieux lutter contre la fraude fiscale ou la fraude sociale ou de détecter, par exemple, qu'un élève risque de rencontrer des difficultés dans son parcours scolaire et mériterait une attention particulière. Le *datawarehouse* et le *datamining* permettront de mieux cibler, profiler et détecter les individus, et donc de leur appliquer des décisions particulières.

Un autre élément important de ces réseaux, ce sont les « sources authentiques ». Certaines bases de données sont créées sous la responsabilité d'une administration particulière, et ces sources authentiques vont garantir aux autres administrations la fiabilité de certaines informations de base.

Voilà l'état du développement du gouvernement électronique et les défis posés par les interconnexions qui augmentent la puissance de l'administration publique. Face à une telle situation, que dit le droit belge ?

Le droit belge suit l'article 8 de la Convention européenne de sauvegarde des droits de l'homme, lequel consacre la vie privée et prévoit, dans son alinéa 2, que des ingérences des autorités publiques dans la vie privée sont possibles, à condition qu'elles soient prévues par la loi et nécessaires à la sécurité nationale et publique.

Le fondement même du droit à la vie privée éclairera le droit belge. L'article 8 précité trouve un écho dans l'article 22 de la Constitution. Celui-ci

introduit une précaution supplémentaire, en ce sens qu'il reprend le contenu de l'article 8 et la possibilité d'ingérence, mais en précisant que ladite ingérence doit nécessairement être fondée sur une loi formelle, c'est-à-dire votée par un pouvoir législatif.

Ces lois peuvent être par exemple des décrets de la Communauté française, la Région wallonne ou la Région flamande. Ce peut être aussi des lois fédérales. L'idée est de dire que s'il faut une ingérence dans la vie privée, elle ne sera autorisée qu'au terme d'un débat démocratique.

L'article 8 de la Convention européenne de sauvegarde des droits de l'homme, contient les deux exigences que nous avons vues poindre dans la décision du tribunal constitutionnel.

La première exigence est celle de la **proportionnalité**. C'est sur ce point qu'en Belgique et qu'au sein de la commission de la protection de la vie privée les décisions manquent le plus. La proportionnalité exige qu'il y ait un raisonnement établissant les intérêts en présence. Quel est, d'une part, l'intérêt de la personne à voir protéger sa confidentialité et, d'autre part, quel est l'intérêt de l'État à pouvoir utiliser telle ou telle donnée? L'efficacité administrative n'est pas un gage de proportionnalité.

Je cite pour exemple une décision récente de la commission de protection de la vie privée qui m'apparaît aller beaucoup trop loin. À propos d'octroi d'allocations sociales pour handicapé, la loi se réfère à des conditions de revenus. On en tire comme conséquence qu'il est légitime que l'administration des handicapés ait un accès d'office sans s'inquiéter préalablement de l'avis de la personne concernée à la base de données fiscales. On pourrait imaginer qu'un contrôle de proportionnalité amène des possibilités de contrôle *a posteriori* et pas nécessairement des vérifications *a priori* et que l'on recherche avec les administrations s'il n'y a pas d'autres manières d'obtenir le même résultat par des voies moins attentatoires à la vie privée, ne serait-ce que par une information préalable doublée d'une possibilité de opt out. La Cour constitutionnelle insiste là-dessus dans sa condamnation d'un décret de la Communauté flamande qui pour prévenir et sanctionner le dopage avait prévu la publication sur Internet du nom des sportifs condamnés pour dopage. Cet arrêt annule le décret flamand et exige qu'on utilise la voie la moins attentatoire et le minimum de données nécessaire.

La deuxième exigence est celle de la **transparence**. Elle a été totalement traduite dans le cadre du système d'informations Phenix. On y a repris telles quelles les exigences de transparence fixées par l'arrêt Rotaru de la Cour européenne des droits de l'Homme, qui date de 2001. Il y est mentionné que, si une administration veut utiliser des données à caractère personnel ou faire un traitement, c'est-à-dire s'ingérer dans la vie privée, une loi est indispensable. Chez nous, l'article 22 de la Constitution restreint la possibilité d'ingérence à l'existence d'une loi au sens formel du terme. La législation doit donc préciser une série de critères pour que l'individu puisse savoir, rien qu'à la lecture du texte de la loi, quelle finalité poursuit le traitement, quelles catégories de données sont reprises, qui peut y avoir accès, quelle est la durée de conservation,... Ce sont toutes des exigences de transparence importantes.

Au-delà de cette transparence par la loi, se pose d'autres questions suite à l'affirmation progressive du principe de la « *collecte unique* », suivant lequel une information déjà présente dans une source authentique ne doit plus être réclamée aux citoyens. Ainsi, l'article 22 de la loi du 16 janvier 2003 portant création d'une Banque-carrefour des entreprises affirme que « *Des autorités, administrations et services qui sont habilités à consulter les données de la Banque-carrefour des entreprises, ne peuvent plus réclamer directement ces données aux entreprises... Dès qu'une donnée est communiquée et enregistrée dans la Banque-carrefour des entreprises, les services habilités à consulter ces données, ne peuvent plus, si ces données ne leur sont pas communiquées directement, en imputer la faute à l'intéressé.* ». Cette première traduction devrait être généralisée à d'autres sources authentiques dans lesquelles il sera permis aux autorités de puiser allégrement et ce dans le cadre de l'application d'une législation sans plus demander que le citoyen communique lui-même partie ou l'ensemble des informations nécessaires à l'application de la législation.

Ainsi, l'administration fiscale pourrait-elle trouver, dans un premier temps, auprès de l'administration de la population : la composition du ménage, auprès de l'administration de la sécurité sociale, directement les données de revenus, dans un deuxième temps, auprès de la Banque carrefour des entreprises : les différentes fonctions exercées par le contribuable comme dirigeant ou administrateur d'entreprise, et auprès d'autres administrations, dans un troisième temps, bien d'autres informations comme son passé d'employé, les voitures immatriculées à son nom, etc. Sans doute, l'efficacité administrative y trouve son compte ! Par contre, le citoyen s'inquiète à juste titre de l'absence de transparence du fonctionnement que ces connections inter-administrations

engendrent. Ces citoyens pourraient ignorer les informations collectées ailleurs, informations sur lesquelles l'administration fonde précisément sa décision. Il est donc important que l'administration qui utilise de telles données en provenance de sources authentiques externes informe le citoyen de sa détention de telles données et indique le contenu de celles-ci afin de permettre au citoyen la contestation sur le contenu ou la qualité des données ainsi obtenues voire sur la légitimité des traitements qui sont à la base d'une telle détention.

Pour certains, le choix doit être laissé au citoyen, soit de fournir lui-même les données ainsi visées, soit de consentir à leur accès auprès d'une source authentique. C'est la voie suivie en France, si on examine la portée de certains articles de l'ordonnance du 7 décembre 2005 qui instaurent au profit du citoyen ce droit alternatif. En particulier, l'article 7 de l'ordonnance précise : « *Il est créé un service public, exploité sous la responsabilité de l'Etat, consistant en la mise à disposition de l'usager d'un espace de stockage accessible en ligne. Cet espace, placé sous le contrôle de son titulaire, ouvert et clos à sa demande, permet à l'usager de conserver et de communiquer aux autorités administratives des informations et documents utiles à l'accomplissement de ses démarches.* ». Deux modèles peuvent en effet conduire l'évolution des relations entre l'administration et le citoyen dans le cadre de l'utilisation des technologies nouvelles.

Un premier modèle conçu sur le mode du « **benevolent government** » entend donner à l'administration le pouvoir d'utiliser toutes les ressources des technologies pour faciliter la vie du citoyen et l'exercice de ses droits : ainsi, le citoyen qui entre dans les conditions de l'application d'une réglementation devrait sans démarche même de sa part pouvoir être repéré par l'administration et bénéficier automatiquement des avantages qui lui sont dus. Le pensionné disposant de revenus modestes et ayant un enfant handicapé serait automatiquement allocataire de la prime que lui réserve telle ou telle législation, l'administration ad hoc se chargeant de collecter auprès des autres administrations l'information nécessaire pour identifier les destinataires des droits.

Par opposition à ce modèle, celui du « **citizen's empowerment** », conçoit les technologies de l'information d'abord comme un outil au profit du citoyen qui mieux informé et disposant de ses propres outils d'accès à l'information peut plus facilement introduire ses requêtes et dialoguer avec l'administration pour obtenir le bénéfice de ses droits. Comme le note G. CHATILLON à propos de l'ordonnance française de décembre 2005, « *ce coffre fort numérique personnel*

*de l'utilisateur peut devenir, mais uniquement si l'utilisateur y consent, un espace de travail collaboratif entre l'utilisateur et l'administration. En effet :*

*1) l'utilisateur est en droit d'autoriser l'administration à puiser dans les documents entreposés pour alimenter les téléservices administratifs. La fonction de "back office" c'est à dire de traitement automatisé des données personnelles des usagers par les divers services publics chargés des téléprocédures et des téléservices est ainsi transformée : l'utilisateur participe de lui-même à ces opérations, les déclenche et en contrôle l'usage.*

*2) l'utilisateur peut utiliser ce nouvel espace de travail collaboratif pour autoriser l'administration à y entreposer des documents. On trouve alors dans le même espace numérique des documents personnels de l'utilisateur et des documents administratifs. Rien n'empêche alors que cet espace permette le traitement des "dossiers" communs à l'utilisateur et à l'administration. Le "dossier administratif en ligne" prend forme. ».*

L'actualité de l'administration électronique à la mode belge oblige à dire quelques mots sur l'existence de réseaux sectoriels au sein desquels existent des règles particulières de circulation de l'information et des méthodes appropriées de contrôle des flux par des autorités de contrôle créés au sein de ces réseaux.

Evoquer les réseaux sectoriels c'est parler de la Banque-carrefour de sécurité sociale (en abrégé : BCSS), fondée en 1990. Cette banque se présentait à la fois comme un outil de gestion et de contrôle des flux réalisés entre tous les organismes belges publics et privés intervenant en matière de sécurité sociale (ils sont plus de 50) et comme un outil de contrôle des communications entre le secteur de la sécurité sociale et le reste des administrations.

Il s'agissait là d'une institution facilitant les flux intra-sectoriels mais également les sécurisant et les contrôlant via les décisions d'un comité sectoriel, distinct de la Commission de protection de la vie privée, une sorte de gouvernance des réseaux pour reprendre le terme de Pierre Trudel.

Ce précédent fait aujourd'hui recette. Se multiplient les réseaux sectoriels, celui de la justice (Phénix), celui de la santé (e-Health) celui de l'économie et de l'emploi (la Banque carrefour des entreprises (BCE)), celui pressenti des Finances (COPERFIN). L'idée est, à l'intérieur même de l'administration fédérale, de maximiser les échanges d'informations entre des instances administratives ayant en charge un domaine commun d'activités en dotant ces

réseaux sectoriels d'une véritable autorité de contrôle. Les finalités de tels réseaux sont multiples : outre d'assurer la correcte application des règlements, il s'agit de doter les administrations, au sein et grâce à ces réseaux, d'outils puissants d'aide à la décision, de contrôle de la correcte application des législations, de systèmes de gestion de risque, etc.

L'article 31bis de la loi relative à la vie privée du 8 décembre 1992, tel qu'introduit par la loi du 26 février 2003, institue la possibilité de création, au sein de la Commission de la protection de la vie privée, de comités sectoriels compétents pour instruire et statuer à propos de demandes relatives aux traitements ou aux communications de données faisant l'objet de législations particulières. Ainsi, sur le modèle du comité de surveillance de la Banque-Carrefour de la sécurité sociale, ont été créés les comités sectoriels du Registre national, de la Banque-Carrefour des entreprises, de l'autorité fédérale et le comité de surveillance dans le secteur judiciaire dans le cadre du projet Phénix. S'ajouteront sans doute des comités de surveillance en matière de télémédecine, en matières statistiques et fiscales, etc.. On ajoutera que l'article 36bis de la loi du 8 décembre 1992 institue au sein de la Commission de la protection de la vie privée un comité sectoriel dit « pour l'autorité fédérale », compétent pour « toute communication électronique de données personnelles par un service public fédéral ou par un organisme public, avec personnalité juridique qui relève de l'autorité fédérale. »

Chaque comité sectoriel est composé paritairement de trois membres de la Commission ainsi que de trois membres externes désignés par la Chambre des représentants.

Il dispose, alors que la Commission ne se voit gratifiée que d'un pouvoir d'avis ou de recommandation, d'un pouvoir d'autorisation en ce qui concerne les flux relevant de sa compétence. La protection des citoyens à l'égard de ce pouvoir d'autorisation des destinataires des données en cas de contestation sur la légitimité d'un refus ou d'une autorisation d'un traitement pose question, dès lors que la possibilité d'introduire un recours au Conseil d'Etat est discutable et qu'aucun autre recours n'est organisé par une disposition particulière.

Les avantages du système sont connus : la composition paritaire des comités permet une meilleure spécialisation voire expertise des membres, une meilleure connaissance des besoins de l'administration et surtout un contrôle plus effectif des flux en question. L'intervention *a priori* de ces comités permet une meilleure protection des citoyens.

On relèvera avec D. De Bot qu'il est cependant à craindre que la proximité du terrain renforcée par le fait que chaque comité est « flanqué » d'une institution

de gestion du secteur concerné, qui prépare l'avis technique et juridique relatif au dossier introduit par cette dernière, favorise en définitive une plus grande complicité avec les administrations chargées par ailleurs d'instruire le dossier. Par ailleurs, la multiplication des comités sectoriels peut amener, outre une dilution des responsabilités, une diversité des jurisprudences. On ajoutera que la multiplication des flux entre administrations relevant de comités sectoriels distincts entraînera de délicats problèmes de partage des compétences entre les différents comités sectoriels. Enfin, il n'est pas évident qu'une vue globale et la définition de principes généraux valables pour l'ensemble de l'administration publique soient encore possibles.

Sans doute, cela dépendra, d'une part, des synergies qui seront créées entre ces comités sectoriels et, d'autre part, de la cohésion que pourra maintenir entre l'action de ces comités la Commission dont ils relèvent tous. Peut-être eût-il été suffisant de mettre en place au sein de ces administrations ou de ces secteurs administratifs un « préposé » à la protection de la vie privée et de prévoir l'intervention de celui-ci pour certains dossiers en même temps que l'obligation d'informer la Commission et que la possibilité de saisir la Commission ou, pour cette dernière, la possibilité de se saisir de tout dossier.

A chaque réseau donc, son comité sectoriel... Sans doute, celui-ci est formellement rattaché depuis une loi de 2003 à la Commission de protection de la vie privée mais son fonctionnement le rapproche du terrain à contrôler, et ce au risque d'un affaiblissement des principes de la protection des données.

J'aurais aimé vous faire part d'autres remarques sur les choix belges : la carte d'identité électronique et le numéro de registre national, numéro d'identification unique, mais le temps qui m'est imparti étant limité, j'évoquerai donc pour conclure les compétences de la Communauté française en matière de protection des données et lui adresserai un message.

Dans l'excellente revue qui nous a été distribuée, je suis surpris qu'il ne soit pas fait mention des développements du gouvernement électronique dans l'administration de la communauté française. Je sais qu'elle est inchoative et qu'une cellule ISA a été mise en place, de la même manière qu'EASI-WAL en Région wallonne ou la Fedict au niveau fédéral. En Région bruxelloise, un système est également établi.

De plus en plus de dossiers méritent une attention particulière de la Communauté française en ce qui concerne la protection des données. Un décret récent de la Région flamande rappelle que tout ce qui relève de la

politique de santé implique la mise sur pied de systèmes d'information. Dans l'enseignement, on se retrouve régulièrement confronté au traitement de données relatives aux étudiants en difficulté, aux diplômés, aux transferts et à la mobilité des étudiants. Toutes ces questions doivent faire l'objet d'une attention particulière et d'un encadrement de la part de la Communauté française.

Il me semble dès lors essentiel que la Communauté française marque un intérêt particulier à la protection des données. Elle en a la compétence. Un arrêt de la Cour constitutionnelle du 12 mars 2008 le dit clairement. Il est certain que dans le cadre des compétences qu'une Communauté exerce, elle doit veiller au respect de la protection des données. L'arrêt ajoute que la loi du 8 décembre 1992 en matière de protection des données constitue à cet égard-là une réglementation minimale pour assurer cette protection. Un tel arrêt constitue un appel évident à la prise de responsabilité de la Communauté française en matière de protection des données. Il est fondamental qu'elle s'intéresse à la façon dont les interconnexions se font à l'intérieur de ses administrations, à la manière dont s'effectuent un certain nombre de traitements et la prise de décisions, et qu'elle se dote en toute autonomie d'une instance de contrôle, véritablement indépendante. Une telle politique me paraît essentielle dans notre Communauté et ce afin que puisse se développer une véritable confiance entre le citoyen et l'administration.

**M. Dechamps, modérateur,** Rédacteur en chef de Citizen<sup>e</sup> – Monsieur Poullet, je vous remercie pour cet exposé. Vous avez déjà soulevé de nombreuses questions. Quelques autres vous seront posées par les participants avant la pause.

**M. Dechamps, modérateur,** Rédacteur en chef de Citizen<sup>e</sup> – La parole est à M. Verschuere, Président de la Commission de la protection de la vie privée.

## **2. Pédagogie, assistance et contrôle : les missions de la Commission de la protection de la vie privée au bénéfice des services publics**

■ **M. Verschuere, *Président de la Commission de la protection de la vie privée***

– Ce matin, en réfléchissant à ce que j'allais vous dire, j'ai choisi de vous faire un exposé informel plutôt qu'une description rigoureuse du fonctionnement, des compétences et des pouvoirs de la Commission de la protection de la vie privée. Vous trouverez aisément toutes ces informations sur le site Internet de cette commission. Je ne pense pas que ces renseignements doivent faire l'essentiel des débats qui se tiennent aujourd'hui dans cet hémicycle.

C'est la troisième fois que le parlement de la Communauté française organise un débat dans le contexte de la semaine de l'Internet, et je ne puis que m'en réjouir. La première journée a été consacrée aux logiciels libres et aux services publics indépendants, la deuxième aux services publics et à la mutualisation informatique, de la théorie à la pratique. Aujourd'hui, nous parlerons du traitement et de la protection des données des administrations.

J'établirai d'abord un constat : il me semble que l'on a mis la charrue avant les bœufs. Les services publics et la mutuellisation informatique, pour quoi faire ? Les logiciels libres et les services publics indépendants, pour quoi faire ?

Le véritable problème actuellement n'est pas de savoir ce que fait la Commission de la vie privée ou de savoir comment fonctionne un service régional ou fédéral qui a en charge l'informatisation, mais de connaître leur but, les moyens dont ils bénéficient et la justification de leur objectif.

Pour répondre à cette question théorique, j'ai parcouru l'ensemble des numéros de la revue *Citizen-E* et le résultat est assez surprenant. Cette revue m'a permis de prendre connaissance d'une série d'articles portant sur des enjeux desquels on ne savait pas à qui ils s'adressaient et pourquoi ils existaient. On peut découvrir la création de nouveaux logiciels, de nouveaux intégrateurs, de nouveaux contre-intégrateurs et contre-logiciels initiés par d'autres pouvoirs publics. On peut aussi découvrir des plates-formes qui devraient, dit-on, enfin mutualiser les enjeux alors que précédemment il existait des plates-formes réunissant 14 ou 127 communes. Mais se focaliser sur les enjeux techniques et technologiques ne constitue pas le vrai débat dans une société démocratique.

Je dirai un mot sur la proportionnalité. L'efficacité administrative est ce qui est mis en avant pour justifier le développement considérable, voire anarchique, des technologies de l'information dans les services publics. Mais sur quels critères peut-on l'évaluer ? On avance parfois le bien des usagers. Certes, c'est mieux que les trains arrivent à l'heure, qu'ils ne déraillent pas, etc. Mais de quel bien parle-t-on ? Avec l'enjeu du développement technologique, on a perdu le sens de la mission à travers laquelle on doit conduire l'action publique. On aurait peut-être dû réfléchir davantage à évaluer la nécessité de ce développement et à la manière dont il fallait l'opérer.

Je vais illustrer mon propos d'une façon qui vous paraîtra peut-être impertinente. En couverture du dernier numéro de *Citizen-E*, sous ma photo, il est écrit : « Corve, sur la voie de la protection de la vie privée ». À la fin de l'article, Geert Mareels conclut : « Aujourd'hui l'administration flamande n'accède aux données d'un individu que lorsque celui-ci veut faire un usage d'un droit particulier. C'est ainsi que, si un citoyen demande une bourse d'études, le fonctionnaire vérifie si l'intéressé entre en ligne de compte et peut donc demander des renseignements relatifs à la composition de ménage, aux revenus, etc. » C'est un peu l'exemple que donnait Yves Pouillet avec les

handicapés. Geert Marrels poursuit : « Mais il serait évidemment bien plus pratique [plus efficace au sens d'efficacité administrative] si l'administration pouvait déterminer à l'avance les bénéficiaires potentiels en fonction de leurs droits. Or c'est impossible aujourd'hui puisque l'administration ne peut consulter l'ensemble de ces données. »

Voilà le cœur du débat que nous devons mener. La question n'est pas de savoir ce que fait la Commission de la vie privée. En réalité, aujourd'hui nous devons répondre à la question que pose Geert Mareels de manière assez abrupte. Ce n'est pas une question secondaire dans la mesure où il y a des responsables administratifs du développement technologique rigoureux dans une entité fédérée qui se demandent s'il ne serait pas utile et efficace pour l'administration de tout savoir sur tout le monde.

Quelles questions s'est-on posées avant de formuler de telles affirmations ?

Une autre citation de la même revue, tout aussi problématique, cerne bien l'enjeu de notre réflexion. Le responsable du Réseau santé wallon dit : « En matière de protection de la vie privée, les trois futurs réseaux régionaux attendaient qu'un expert, désigné par le Service Public Fédéral, produise un canevas conforme aux exigences de la législation. Nous l'avons reçu ; le SPF diffuse actuellement la première ébauche de règlement relatif à la protection de la vie privée. Nous attendons également la confirmation que les critères de labellisation des logiciels de médecine générale répondent bien à l'intégration au Réseau santé en 2008. La question est maintenant en suspens. La commission télématique du SPF ne se réunit plus. Nous attendons la poursuite de cette expertise sur les exigences de la réglementation et nous ne pouvons plus travailler. »

Je ne veux pas dire que les administrations collaborent mal entre elles et qu'il faudrait une plate-forme de collaboration entre les experts administratifs qui labellisent les bonnes et les mauvaises pratiques en matière de protection de la vie privée. J'ai repris cette seconde citation parce que le problème est là, il est dans le regard porté sur la Commission de la vie privée, sur son rôle et sur celui qui lui a été historiquement attribué. Or, cette commission est là non pour juger, sanctionner ou freiner la pratique administrative, mais bien pour l'accompagner.

Il est assez saisissant que deux responsables administratifs de grands projets d'informatisation concernant des données très sensibles fassent de telles

déclarations, sans avoir jamais consulté la Commission de la vie privée ni demandé son opinion. La question à se poser n'est-elle pas plutôt la suivante : même s'il n'y avait pas de loi, pas d'article 8 de la Convention, pas de directive européenne, la protection de la vie privée ne serait-elle pas un véritable enjeu démocratique dont l'ensemble des responsables administratifs de ce pays devraient se saisir ?

La question fondamentale est moins un problème de loi, qu'il faut respecter ou parfois changer, que de fond : que veut-on faire de l'informatisation des services publics, à quoi ou à qui sert-elle, vers quoi la conduit-on, quel bénéfice le citoyen en retire-t-il ? Si le citoyen en retire un bénéfice, dans quelle mesure a-t-il participé au débat qui lui aurait permis de comprendre ce qui se passe et de déterminer ce qui se produira à l'avenir ?

L'essentiel est là. Ma présence récente à la commission me permet quelque impertinence. Des responsables administratifs se sont dit : « La vie privée, on sait ce que c'est, on ne va pas perdre de temps à demander l'avis de la commission ».

Cela peut prendre deux semaines, voire un mois, il est vrai, mais qu'est-ce au regard d'un projet qu'on implante à long terme pour guider la démarche administrative et qui concerne bien plus de personnes que deux responsables de service qui craignent de perdre trop de temps ?

Loin de moi l'idée de critiquer toutes les administrations. Je sais – et cette journée en est la preuve – que certains services réfléchissent aux enjeux de la protection de la vie privée. La question essentielle ne porte pas sur les moyens techniques, les logiciels, l'investissement technique mais bien sur les raisons pour lesquelles on a décidé d'informatiser. La question des logiciels libres, des standards, de la mutualisation, etc. passe aussi par une réflexion sur la manière dont on met la technologie à la disposition des utilisateurs.

Je voudrais faire une brève remarque sur les caméras de surveillance qui créent l'émoi et suscitent la polémique. Une loi a même été votée. Elle nous fait entrer collectivement dans la maîtrise démocratique des enjeux. C'est le rôle de la commission que je représente ici. Les citoyens sont plus sensibles aujourd'hui qu'hier à la présence des caméras de surveillance. Cette question fondamentale doit être débattue au même titre que le développement des technologies de l'information et de la communication et de l'informatique au service de l'administration. On dit souvent que la propension d'une

communauté à reconnaître l'existence d'un risque est déterminée par sa conviction qu'il existe des solutions. Si elle pense qu'il n'y a pas de solutions, elle imagine souvent qu'il n'y a pas de risques. On ne trouvera pas de solutions si on ne s'interroge pas sur ce que l'on fait, pourquoi on le fait et au bénéfice de qui. On peut développer les technologies de l'information et se plaindre que tout le monde n'ait pas accès à Internet tout en constatant que ceux qui y ont accès sont surveillés par Google. Le monde est complexe et les problèmes se juxtaposent sans que nous n'y voyions de solutions et sans que nous ne nous donnions les moyens de les maîtriser. Du coup, on pense aussi qu'il n'existe pas de risques réels

La Commission de la vie privée n'est pas un frein au développement technologique. Elle est composée majoritairement de juristes occupés la plupart du temps à faire des mathématiques, du droit et de la philosophie. Experts de la discussion critique, ils se veulent les vigiles des enjeux pour donner le signe que la résistance critique aux innovations technologiques est en soi un but légitime et nécessaire.

Espérer annuler les résistances et les critiques est illusoire. Leur disparition signifierait la fin même de la technologie comme moteur d'une transformation technique réfléchie de la société. La résistance critique aux technologies fait partie intégrante de la force transformatrice qu'elle semble combattre. Elle est aussi nécessaire à la transformation de la société que ne l'est le circuit de refroidissement au moteur d'une voiture.

Nous avons déjà eu un débat sur les caméras de surveillance et nous en aurons d'autres. À Reykjavik, il n'y a pas eu de débat, pourtant il y a des caméras partout. Elles sont même sur les chaînes publiques. Il suffit d'allumer sa télévision pour voir ce que filment les caméras de la police. On peut même surveiller son propre jardin ou celui de son voisin. L'absence de débat critique nous conduit à un enfermement dont on ignore encore où il peut mener.

Mais de quoi devons-nous débattre exactement ? De la vie privée, certes, mais qu'est-ce que cela signifie ? On ne sait pas très bien. Je lisais récemment dans la presse que l'Union des villes et des communes flamandes trouvait que la législation fédérale sur la vie privée était insupportable et empêchait les communes de fonctionner. S'est-on demandé de quoi l'on parle ? Non. Parle-t-on de la vie privée ? Pas exactement. On parle plutôt du développement des technologies, du droit et de la liberté des personnes de se déplacer, de penser, d'être dans le monde.

Selon Pascal, le grand malheur de l'homme était de devoir sortir de sa chambre et de ne pouvoir y rester. Le défi est de garantir la liberté individuelle dans la vie publique et collective malgré le développement des technologies de l'information. La question n'est pas de savoir si la loi fédérale est trop stricte puisqu'elle ne dit rien à ce sujet. Elle parle de proportionnalité mais j'ignore réellement ce que cela signifie. Elle parle de loyauté, de licéité, de détermination, de prévision raisonnable, d'adéquation, de pertinence, de non-excessivité, de nécessité... autant de concepts dont personne ne pourrait dire, sans les avoir confrontés concrètement aux réalités, ce qu'ils veulent dire et ce que l'on va en faire.

Donner du contenu à la nécessité est bien notre mission d'aujourd'hui. On peut commencer. Selon Yves Poullet, il ne faut pas utiliser les données plus que nécessaire. Selon la loi, le traitement doit être nécessaire et les données doivent être simplement adéquates, pertinentes et non excessives. J'en conclu qu'elles peuvent être simplement utiles. Il faut débattre. Les administrations doivent aborder le sujet. Elles sauront alors ce qu'elles font, ce qu'elles maîtrisent et où elles vont. Cette journée est l'heureux présage de cette dynamique qui aurait sans doute dû être enclenchée avant qu'on ne se pose la question de la normalisation technique des logiciels, des standards, des mutualisations, des logiciels libres ou non.

**M. Dechamps, modérateur**, Rédacteur en chef de Citizen<sup>e</sup> – La parole est M. Quintin, Administrateur général adjoint de la Banque Carrefour de la sécurité sociale...

**M. Verschuere**, Facultés Universitaires Notre-Dame de la Paix (FUNDP) – La Banque Carrefour de la sécurité sociale est le meilleur contre-exemple de réflexion intégrée et raisonnée que je viens d'évoquer...

### **3. Présentation générale du modèle de la « Banque Carrefour »**

**■ M. Quintin, Administrateur général adjoint de la Banque Carrefour de la Sécurité sociale**

– Après ces exposés sur les défis liés au respect de la vie privée, je me présente comme un responsable d’une institution publique de sécurité sociale qui doit faire fonctionner son administration sociale de manière efficace et efficiente et dont les acteurs sont nombreux.

Avec de bons principes et des moyens organisationnels, juridiques et techniques suffisants, une administration peut relever le défi d’une protection réelle de la vie privée, tout en étant efficace et efficiente pour les assurés sociaux et tous les acteurs du secteur du secteur social qui sont nos clients.

Je souhaiterais excuser M. Robben, Administrateur général, que je remplace au pied levé.

Je tenterai donc de vous expliquer comment le modèle d’organisation de la Banque Carrefour de la sécurité sociale (BCSS) peut concilier équitablement le respect des principes de protection de la vie privée avec une gestion efficace d’une administration chargée de simplifier la vie administrative et d’automatiser le plus largement possible la fixation et le calcul des droits et obligations en matière de cotisations et d’allocations sociale.

La BCSS a été créée par une loi du 15 janvier 1990 qui définit les principes de son modèle d'organisation.

Elle est avant tout un échangeur de données électroniques efficace et dûment sécurisé. Elle profite de cette automatisation pour intégrer dans les activités administratives des personnes et des acteurs en présence par un effort de réingénierie et d'optimisation des processus.

L'organisation de cet échange de données respecte le « principe des silos » présenté par M. Pouillet. Lors de la création de la Banque Carrefour de la sécurité sociale en 1990, le concept d'une banque de données sociales centralisée qui aurait intégré toutes les données sociales nécessaires par exemple pour la fixation et le calcul des allocations de chômage, des pensions ou des allocations familiales a été écarté d'emblée. C'eût été techniquement faisable puisque les données sur lesquelles reposent ces calculs sont largement identiques au sein de toute la sécurité sociale: pensons par exemple aux notions de composition de famille, revenus et temps de travail, état de santé ou statut social !

Mais la loi organique sur la Banque Carrefour de la sécurité sociale dispose le contraire : elle impose le respect de l'autonomie et des compétences des institutions de la Sécurité sociale tout en les intégrant par la mise en place d'un réseau d'échange d'informations. Tout cela doit se faire sans qu'il y ait d'enregistrement de données sociales à caractère personnel dans les banques de données de la Banque Carrefour de la sécurité sociale. Ces dernières ne sont qu'un ensemble de pointeurs fédérés dans ce que nous appelons notre répertoire des références qui ne comprend aucune information de contenu.

Pour construire cet ensemble de services, nous avons respecté quelques principes importants liés à la modélisation des informations sous forme factuelle, leur collecte unique, leur réutilisation, les principes de bonne gouvernance, l'échange électronique selon des mécanismes push et pull, la sécurisation de l'information et la protection de la vie privée.

J'ai lu hier les quarante-trois pages du récent accord gouvernemental. Quels sont les concepts qui y reviennent systématiquement ? On y mentionne la simplification administrative, l'automatisation des droits, la simulation de l'évolution de ses droits et obligations sociales compte tenu de l'évolution que l'on souhaite donner à sa vie professionnelle, l'efficience et l'efficacité des services publics. Cela témoigne d'un ensemble d'attentes des utilisateurs du

secteur social qui veulent une protection sociale, pro-active, efficace et efficiente ainsi que des informations statistiques intégrées. Le gouvernement souhaite que la sécurité sociale dispose d'un outil permettant la mise en œuvre de ces différents concepts. C'est pour ces objectifs que nous avons développé un ensemble de services informatiques permettant d'obtenir les bonnes données sociales, au seul moment nécessaire et pour la seule personne concernée ; ces services sont fournis par le réseau de la Banque Carrefour de la sécurité sociale sur base de la collaboration réciproque de tous les institutions de sécurité sociale.

Je reviendrai sur la remarque de M. Verschuere sur l'automatisation des droits. C'est un grand enjeu puisqu'ils pourraient, avec les technologies de l'information, être systématiquement automatisés. À la naissance de mon enfant, dois-je encore demander une allocation familiale, comme c'est encore le cas pour le moment, ou pourrais-je la recevoir automatiquement ? C'est un enjeu politique, surtout dans les secteurs de l'aide et de la protection sociale offertes par notre système social. Systématiquement se pose la question de savoir si la personne doit encore demander et prouver qu'elle peut obtenir un droit ou si, sur la base de l'information dont peut disposer le réseau de la Banque Carrefour de la sécurité sociale, le droit peut lui être accordé automatiquement.

La réponse figurant dans les réglementations sectorielles n'est absolument pas homogène. Certaines imposent l'automatisation du droit. Par exemple, la dernière réglementation sur l'application des tarifs sociaux en matière de distribution et de production d'électricité impose l'automatisation de ce droit. Cela signifie que la Banque Carrefour de la sécurité sociale doit communiquer certaines informations sociales et relatives à la composition du ménage au SPF Economie, qui à son tour va transmettre l'information pertinente aux fournisseurs d'électricité ou de gaz. Cela dispense le citoyen d'introduire une demande et de prouver à son distributeur qu'il remplit bien les conditions requises pour bénéficier d'un tarif social. La loi nous impose ainsi de transmettre automatiquement certaines informations à caractère personnel à des partenaires privés. Et cela nécessite bien évidemment la mise en place d'une architecture de communication ainsi que de filtres de privacy qui font en sorte qu'un fournisseur d'électricité doive lui-même nous poser la question sur le fait de savoir si son client peut bénéficier du tarif social et que nous ne lui répondions que par un simple « oui » ou « non ». Tout l'art du réseau de la Banque Carrefour de la sécurité sociale consistant à orchestrer l'échange d'informations personnelles en son sein (composition de ménage, statuts des personnes – e.a. personne handicapée, bénéficiaire du revenu d'intégration

sociale et/ou bénéficiaire d'intervention majorée dans les soins de santé, le cas échéant niveau des revenus, etc..) pour finalement ne communiquer au destinataire qu'une seule information la plus neutre que possible, à savoir : cette personne peut ou non bénéficier du tarif social.

D'autres réglementations prévoient de ne répondre que sur demande de l'assuré social. Ainsi, il faut toujours introduire une demande d'allocations familiales, alors que ce droit pourrait parfaitement être automatisé sur la base de la composition du ménage, des cotisations de sécurité sociale payées et de l'inscription d'un nouveau-né au registre national. Il suffirait aussi de consulter les fichiers de la Direction générale des personnes handicapées pour octroyer des allocations familiales majorées aux enfants handicapés. Et ainsi de suite.

Des principes fondamentaux doivent toujours être respectés pour garantir une réelle protection de la vie privée.

Le principe de la collecte unique et la réutilisation de l'information appartient à ces fondamentaux de la privacy. Le réseau de la sécurité sociale a comme clients l'ensemble des institutions de sécurité sociale au sens large (p.e. les secteurs des pensions, des allocations de chômage, des allocations familiales, de l'aide sociale, des services aux personnes handicapées, des maladies professionnelles, des accidents de travail, des soins de santé gérés par l'INAMI et les mutualités). Environ deux mille acteurs participent ainsi au réseau de la sécurité sociale. Nous avons établi une répartition fonctionnelle entre les différentes sources authentiques du réseau. Chaque institution doit veiller à ce que les informations qu'elle détient puissent être largement utilisables pour d'autres fins en sécurité sociale. Grâce à ce système, une information identique ne doit plus être demandée à plusieurs administrations différentes. Si la source authentique gère correctement les informations, l'institution qui souhaite un renseignement ne doit pas le demander au citoyen, elle va le puiser directement à la source authentique. Cela implique une organisation fonctionnelle et une répartition de l'information sociale entre les différents acteurs ; cela implique aussi le respect de contraintes particulières de qualité de l'information détenue par une source authentique..

C'est ainsi que beaucoup de données authentiques qui permettent d'automatiser p.e. des droits dans le secteur du chômage, des soins de santé ou des allocations familiales, proviennent des déclarations des employeurs faites à l'ONSS, par le biais de la déclaration multifonctionnelle (DmfA). Le glossaire d'informations a été profondément rénové afin que les informations

communiquées à l'ONSS puissent être réutilisées pour calculer le plus automatiquement que possible les droits à l'assurance soins de santé ou aux indemnités de chômage. L'ONSS recueille des informations pour effectuer son travail de collecte de cotisations sociales mais en outre, comme il est une source authentique pour certaines données, il est chargé de collecter ces données d'une manière telle qu'elles puissent être utilisées par d'autres partenaires attribuant des allocations sociales. Ce principe de la collecte unique et de la réutilisation de l'information induit des charges importantes pour les sources authentiques qui ont des obligations de tenue à jour de l'information, de transparence vis-à-vis de l'utilisateur et de vérification de la qualité de l'information.

Une fois ces sources authentiques bien établies en fonction d'un modèle de répartition fonctionnelle, il convient de gérer, stocker et normaliser les informations pour permettre leur échange électronique au sein du réseau.

Les informations peuvent donc être envoyées à la Banque Carrefour de la sécurité sociale qui sait qu'elle doit les communiquer à tel secteur intéressé. C'est le modèle push qui est alors mis en œuvre électroniquement. Mais il existe aussi le modèle pull où une institution de sécurité sociale consulte à son initiative des données du réseau. La Banque Carrefour de la sécurité sociale est ainsi un intégrateur de services multiples.

Je voudrais bien sûr prolonger mon exposé en vous précisant les grands principes de sécurisation et de protection de la vie privée que nous avons intégrés dans notre système d'information.

La base en est avant tout une profonde culture de sécurité de l'information qui a été implantée dans toutes les institutions de sécurité sociale. L'amorce et le catalyseur du déploiement de cette culture est l'institution de la fonction de conseiller en sécurité au sein de chaque institution, celui-ci s'en référant directement au fonctionnaire dirigeant restant le responsable final de la politique de sécurité. Le conseiller en sécurité doit notamment établir un plan de sécurité à actualiser chaque année ; il veille à ce que les normes minimales de sécurité émises par la Banque Carrefour de la sécurité sociale soient bien déployées et respectées au sein de son institution. Ces éléments exemplatifs sont inscrits dans la loi organique de la Banque Carrefour de la sécurité sociale ou dans ses arrêtés d'exécution. D'autres instances fédérales, régionales et communautaires s'en sont d'ailleurs inspirées pour fixer des mesures similaires dans leur secteur.

Un autre principe légal essentiel consiste dans le fait que toute communication de données sociales à caractère personnel ne peut se faire que moyennant l'autorisation préalable accordée par le Comité sectoriel de la sécurité sociale et de la santé. Le Comité sectoriel juge en l'occurrence de la finalité des traitements informatiques que nous souhaitons opérer et vérifie que les données à communiquer sont strictement proportionnelles aux finalités poursuivies. Les dossiers que nous soumettons à l'autorisation du Comité sectoriel doivent donc être parfaitement justifiés ; ils comprennent les bases légales et réglementaires fondant la légitimité et la finalité recherchée ainsi que l'inventaire complet des données qui seront communiquées. Ces autorisations d'accès accordées sont évidemment publiques.

Le troisième principe de sécurité consiste dans le contrôle préventif automatisé des échanges d'informations qui s'effectue via ce qu'il est communément convenu d'appeler le répertoire des références de la Banque Carrefour de la sécurité sociale ; il est en quelque sorte le noyau central de nos activités. Ce répertoire des références indique :

- pour chaque citoyen, auprès de quels acteurs du secteur social, il possède un dossier, sous quelle qualité et pour quelle période ;
- pour chaque type d'acteur du secteur social, la qualité sous laquelle un citoyen est connu auprès de cet acteur ainsi que le type de données qui sont disponibles auprès de cet acteur pour chaque qualité ;
- pour chaque type d'acteur du secteur social, la qualité sous laquelle un citoyen peut être connu auprès de cet acteur, les types de données dont cet acteur a besoin et qu'il est autorisé à recevoir d'autres acteurs pour réaliser sa mission.

La Banque Carrefour de la sécurité sociale utilise ainsi son répertoire des références des références pour :

- effectuer un contrôle d'accès préventif, c'est-à-dire limiter l'accès d'un acteur, d'une part, à l'information qu'il peut obtenir et, d'autre part, aux personnes concernant lesquelles il gère un dossier ;
- transmettre des demandes d'informations à l'acteur qui peut fournir l'information ;

- transmettre automatiquement les modifications apportées aux données sociales (p.e. changements d'adresses) aux acteurs du secteur social qui gèrent un dossier relatif au citoyen concerné et qui ont besoin de cette information pour exécuter leurs missions.

Ce répertoire des références contenait au 31 décembre 2007 plus de 125 millions de dossiers. Chaque citoyen y était en moyenne connu auprès de 8,57 acteurs du secteur social.

Une fois l'autorisation accordée par le Comité sectoriel de la sécurité sociale et de la santé, nous intégrons ses paramètres dans ce répertoire des références de telle sorte qu'à chaque communication d'informations entre deux acteurs sociaux portant sur un assuré social, celle-ci soit confrontée préventivement à l'autorisation.

Par exemple, Mr. Dupont est travailleur salarié. S'il a des enfants, il est connu par le secteur des allocations familiales. S'il a eu un accident de travail, il est également connu auprès du Fonds des accidents du travail et des assureurs-loi. Mr. Dupont est bien sûr aussi couvert au regard de l'assurance obligatoire soins de santé et est donc repris dans les dossiers de sa mutualité. Enfin, ses données légales d'identification sont inscrites au Registre national. Notre répertoire des références comprend donc comme données relatives à Mr. Dupont : son numéro d'identification à la sécurité sociale (soit son numéro national, soit son numéro Banque Carrefour de la sécurité sociale s'il ne dispose pas d'un numéro national) et qu'il y a, à son sujet, un dossier disponible sous une certaine qualité auprès de chacune des institutions de sécurité sociales suivantes : à l'ONSS comme travailleur salarié, à l'ONAFS comme attributaire d'allocations familiales, au FAT comme bénéficiant d'une allocation d'incapacité temporaire, auprès des organismes assureurs comme titulaire de l'assurance obligatoire soins de santé, et enfin au Registre national comme résidant en Belgique. Notre répertoire des références sait donc quels types de données sont disponibles pour Mr. Dupont dans ces différents secteurs de la sécurité sociale.

Si maintenant par exemple notre Mr. Dupont perd son travail et souhaite pouvoir bénéficier d'allocations de chômage. Le secteur du chômage devra d'abord l'enregistrer dans notre répertoire des références comme demandeur d'emploi. En fonction des autorisations d'accès qui ont été données structurellement par le Comité sectoriel et qui ont ainsi été paramétrées au sein de notre répertoire des références, l'ONEM et/ou la caisse de paiement

d'allocations de chômage pourront alors soit consulter, soit recevoir automatiquement, selon le cas, les seules données sociales à caractère personnel de Mr. Dupont telles que disponibles pour un demandeur d'emploi auprès de, en l'occurrence, l'ONSS, l'ONAFST, le FAT et le Registre national. Cela permettra à l'ONEM (et à la caisse de paiement d'allocations de chômage que Mr. Dupont aura choisie) d'instruire automatiquement son dossier d'ouverture du droit à et de fixation du montant de l'allocation de chômage.

C'est ainsi que chaque communication de données sociales à caractère personnel est confrontée au répertoire des références. En 2007, ce sont plus de 656 millions d'échanges de données sociales à caractère personnel qui ont été chaque fois contrôlées préventivement, grâce à ce mécanisme du répertoire des références. Il s'agit réellement d'une automatisation des règles les plus fines en matière de protection de la vie privée qui ont été incorporées dans le business même du traitement administratif des dossiers de sécurité sociale.

Je vois que le temps m'est compté ; il y a bien d'autres principes parfois plus techniques qui ont été mis en place pour assurer la sécurité de l'information au sein du réseau de la Banque Carrefour de la sécurité sociale ; je me réfère notamment aux règles en matière de « user access management » ainsi qu'aux loggings sécuritaires permettant de contrôler a posteriori le respect des règles de protection de la vie privée.

Ce modèle de sécurisation de l'information qui est à la base de la Banque Carrefour de la sécurité sociale est ainsi devenu source d'inspiration et de référence dans d'autres secteurs publics au niveau fédéral, régional et communautaire ainsi qu'au niveau européen et international.

J'espère vous avoir convaincu qu'il est possible de concilier une véritable protection de la vie privée avec le principe d'un État social proactif, dynamique et efficient et ce, à l'avantage du citoyen. Cela demande une grande ténacité dans la nouvelle culture d'entreprise y requise, la mise en place de règles organisationnelles et aussi une technologie parfaitement domestiquée. C'est possible, soyez-en convaincus ! (*Applaudissements*)

**M. Dechamps, modérateur**, Rédacteur en chef de Citizen<sup>e</sup> – La parole est à M. Huet, Conseiller en Chef de la Sécurité de l'Information de Fedict, service public fédéral de la technologie de l'information et de la communication.

## 4. Politique nationale de sécurité de l'information : définition des enjeux

■ **M. Huet, Conseiller en Chef de la Sécurité de l'Information du Service public fédéral Technologie de l'Information et de la Communication (FEDICT)**

– Je parlerai d'un sujet plus général que la protection des données de l'administration, à savoir ce que devrait être une politique nationale de sécurité dans un État démocratique moderne.

Je commencerai par une mise en perspective de l'internet. Comme toutes les grandes réalisations humaines, son développement s'est fait par étapes. Au cours de la première étape, que j'appellerai l'âge des pionniers et des rêveurs, durant les années 80 et 90, les bases technologiques ont été jetées ; à cette époque, un certain nombre de penseurs ont dit que l'Internet raccourcirait les distances entre les êtres humains, on a parlé de village mondial, on a dit que l'Internet rendrait l'accès quasi gratuit à la connaissance, qu'il serait un moyen formidable d'expression, qu'il développerait la démocratie, qu'il rapprocherait le citoyen et l'autorité et qu'il ferait tomber certaines barrières au commerce. Tout cela s'est réalisé en grande partie, mais par la suite, des déceptions se sont évidemment manifestées.

Sur le plan économique, il y a eu l'éclatement de la bulle internet. Sur le plan social, on a parlé, et on parle toujours, de la fracture numérique. Et surtout, on s'est aperçu que l'Internet était un formidable moyen à la disposition des escrocs, des extrémistes et des pédophiles. On parle aussi de plus en plus d'espionnage, voire de guerre électronique.

Aujourd'hui, en 2008, on a pris conscience de ces problèmes. On est en train de les résoudre, de telle sorte que, dans un avenir que j'espère proche, naisse le troisième âge de l'Internet, celui de la maturité.

En raison de ces problèmes, le gouvernement a décidé en 2005 la création d'une plate-forme de concertation sur la sécurité de l'information, avec comme premier objectif de faciliter la concertation entre les principales institutions fédérales concernées, ainsi qu'avec les autres niveaux de pouvoir, les entreprises, les consommateurs et les citoyens.

La Commission de la protection de la vie privée, qui dépend du Parlement fédéral, en est membre, ainsi que l'Autorité nationale de sécurité, l'institut régulateur des postes et télécommunications (IBPT), la direction générale « contrôle et médiation » du service public fédéral Economie (qui traite des pratiques commerciales, notamment sur Internet), la police judiciaire (plus précisément la *Federal computer crime unit*), les services de renseignement civil et militaire (la Sûreté de l'État et le Service général du renseignement et de la sécurité, de la Défense), le centre de crise gouvernemental, la Banque-carrefour de la sécurité sociale (qui, comme l'a mentionné M. Quintin, a depuis longtemps mis en place une politique de sécurité pour le secteur de la sécurité sociale), et enfin Fedict, le service public fédéral chargé de promouvoir et de faciliter la mise en œuvre du gouvernement électronique (et qui constitue l'institution de référence du comité sectoriel pour l'administration fédérale, placé sous l'égide de la Commission de protection de la vie privée).

Les experts de cette plate-forme ont élaboré en 2007 une réflexion sur ce que devrait être une politique nationale de sécurité de l'information. Cette réflexion s'appuie sur leur expérience personnelle, ainsi que sur des textes internationaux, notamment des autorités européennes (résolutions, règlements et directives) : une directive en projet sur la protection des infrastructures d'information critiques, des lignes directrices de l'OCDE, ainsi que des rapports de l'agence européenne de sécurité de l'information (l'ENISA).

Il en est résulté un rapport articulé en sept thèmes, allant du plus stratégique, comme l'élaboration d'une stratégie nationale, jusqu'à des thèmes très spécifiques, comme l'organisation de la formation des experts dont le pays a besoin.

Le premier thème est celui de la stratégie nationale. Même si cela paraît évident, les objectifs d'une politique de sécurité doivent être clairement définis. Il

faut donc se poser un certain nombre de questions générales, et y répondre dans le cadre d'un débat démocratique. Il faut décider, par exemple, si la protection de la vie privée est un enjeu important pour le pays : la réponse est évidente dans un État démocratique, mais elle l'est moins pour d'autres questions. Par exemple : le fonctionnement du pays repose-t-il sur des infrastructures d'informations critiques ? Dans l'affirmative, devons-nous définir une politique contraignante en la matière ? Autre question : la politique nationale de sécurité doit-elle englober les entreprises ? Ainsi que les citoyens ? Existe-t-il des enjeux particuliers en matière de commerce électronique ? Le pays dispose-t-il d'une industrie de sécurité que les pouvoirs publics doivent éventuellement épauler, tout simplement pour rester compétitifs avec les pays voisins ?

La réponse à ces questions doit figurer dans une loi-cadre définissant la stratégie nationale, les missions à remplir et leur assignation à des institutions ; et comme l'organisation qui en résulte est relativement complexe, il importe d'en confier la coordination à une autorité.

Le second thème traité par la plate-forme est l'information de la société et la gestion des crises.

Il faut évidemment partir des différentes menaces pesant sur la société.

Nous connaissons depuis longtemps les menaces naturelles et accidentelles que sont les incendies, inondations, tremblements de terre, ..., ainsi que les dysfonctionnements techniques (problèmes d'alimentation électrique, de télécommunication, pannes de matériel, *bugs* logiciels, ...), sans compter les erreurs et négligences commises par le personnel.

Ce qui est nouveau, c'est l'importance prise par les attaques délibérées. Il en résulte évidemment une menace pour la vie privée, mais également sur le plan économique, quand il s'agit des informations confidentielles d'entreprises, secrets industriels ou commerciaux.

En outre, chaque semaine, un certain nombre de sites web sont victimes de défiguration ("*defacing*"), manoeuvre de piratage consistant à modifier le contenu du site dans l'intention de nuire ; le commerce électronique est la cible d'escroqueries en tous genres, et le *netbanking* n'est pas non plus à l'abri.

Citons aussi les *botnets*, des réseaux d'ordinateurs personnels infectés obéissant, tels des zombies, aux ordres d'une organisation criminelle :

aujourd'hui, pour mille dollars par jour, on peut louer de tels réseaux capables de paralyser le site web d'un concurrent, voire le service d'un fournisseur d'accès Internet.

Il ne s'agit pas de menaces théoriques ; notre *Federal computer crime unit* peut citer des cas concrets.

Quels sont les auteurs de ces attaques délibérées ? Il y a dix ans, il s'agissait surtout d'amateurs, de « Robins des bois », qui attiraient gentiment l'attention sur certains défauts. Aujourd'hui, nous sommes surtout confrontés à l'espionnage économique. Je vous invite à lire sur [www.comiteri.be](http://www.comiteri.be) le rapport 2003 du Comité R, l'institution de contrôle des services de renseignement en Belgique (Sûreté de l'État et renseignement militaire). Il est à craindre que, depuis 2003, la situation se soit encore aggravée, comme l'illustre le cas d'officines de renseignement économique qui passent volontiers la ligne rouge.

L'Internet est donc peuplé d'escrocs, d'extrémistes, de terroristes. Il y a aussi une menace d'ordre politique, comme semble l'illustrer la cyber-attaque subie par l'Estonie au printemps dernier ; mais on n'a pas pu en identifier l'origine, ce qui montre bien qu'il est illusoire de faire régner la justice et l'ordre sur internet.

Que faire concrètement ? D'abord protéger les infrastructures critiques. Notre société dépend du bon fonctionnement des télécommunications et de l'informatique. Il faut commencer par définir des critères pour décider de ce qui est critique. Ensuite, il faut en dresser l'inventaire. C'est assez facile pour les pouvoirs publics, mais ce l'est beaucoup moins pour le secteur privé (transports, hôpitaux, télécommunications, etc). Il faut enfin imposer des mesures de sécurité aux propriétaires de ces infrastructures et vérifier leur respect. Très bientôt, la directive européenne évoquée précédemment imposera des obligations en ce sens.

Il faut également mettre en place les moyens aptes à répondre à des incidents majeurs comme l'attaque dont a été victime l'Estonie. De telles équipes d'intervention fonctionnent dans de nombreux pays, avec des dénominations comme *Computer Emergency Response Team* ou *Computer Security Incident Response Team*. Leur première mission consiste à suivre au jour le jour l'évolution des menaces, et à en informer les différents acteurs (institutions publiques, entreprises, citoyens).

Pour obtenir de bons résultats, il est indispensable d'instaurer une collaboration entre les organisations actives dans ce secteur. Voici un exemple de structure nationale de gestion de crise : un centre national collaborant avec ses homologues étrangers, et assistant des centres régionaux ou sectoriels auxquels seraient abonnés les utilisateurs (citoyens, entreprises, pouvoirs publics, etc.).

Le troisième thème de la réflexion de la plate-forme concerne la protection des informations sensibles. Ce concept est défini par la loi et les règlements internationaux auxquels la Belgique a souscrit. On parle dans ce cas d'information classifiée (confidentiel, secret, très secret, etc.). La loi belge précise le type d'informations concernées : plans de défense du pays, missions des forces armées, pérennité de l'ordre démocratique, préservation du potentiel scientifique et économique du pays,... Ceci se retrouve à l'échelon de l'OTAN et de l'Union européenne.

Les grands projets publics se réfèrent de plus en plus à cette notion d'information ou de système sensible. Les composants du projet Galileo, par exemple, devront être certifiés conformément aux règles européennes en la matière.

Certains secteurs constituent des utilisateurs potentiels de ces méthodologies : l'industrie (entreprises "Seveso", secteur nucléaire, ...), le secteur médical (secret médical, garantie de la qualité du matériel), la banque (systèmes de paiement), ...

Cette matière est bien codifiée : les normes et les conventions internationales existent, mais il s'agit d'une matière complexe dont la maîtrise demande des efforts de l'autorité.

Le quatrième thème de réflexion concerne les systèmes de l'autorité. Les services publics qui gèrent de nombreuses informations à caractère personnel ou économique se doivent de donner le bon exemple, et les enjeux financiers sont importants. En particulier, la mise en oeuvre de l'e-government nécessite une coordination de la sécurité entre les différents départements ministériels.

Les normes de la série ISO 27 000 constituent un bon guide pour ce faire. A titre d'exemple, la Banque-carrefour de la sécurité sociale y adhère explicitement, d'autant plus facilement que la loi de 1990 instituant la Banque-carrefour en reprenait déjà de nombreux principes.

Le cinquième thème concerne la délinquance informatique. Il faut évidemment disposer d'un ensemble cohérent de dispositions légales sur la protection de la vie privée, sur les pratiques commerciales, ..., mais de plus, les policiers et les magistrats doivent être sensibilisés et formés à ces questions, et disposer du temps et des moyens nécessaires.

Le sixième thème suit les recommandations de l'Union européenne et de l'OCDE sur la nécessaire collaboration entre les secteurs public et privé. Des groupes de travail internationaux traitent de questions de sécurité pouvant intéresser certaines entreprises, et il est donc essentiel que ces informations soient convenablement relayées.

J'en arrive enfin à la formation. Le pays a besoin d'experts en sécurité de l'information, aussi bien dans le secteur public que privé. Il serait donc utile de définir officiellement un programme de formation en la matière, avec un accent particulier sur les dispositions légales propres au pays. Etant donné qu'il s'agit de matières en constante évolution, il faut mettre en place une concertation permanente entre les secteurs privé et public, ainsi qu'avec les institutions académiques.

\* \* \*

**M. Dechamps** propose un moment de questions-réponses vu l'indisponibilité de M. Quintin l'après-midi.

**M. Verschuere.** – Qu'est devenu le rapport et quelle suite lui a-t-elle été donnée ?

**M. Huet.** – Ce rapport est destiné au gouvernement fédéral. Dans le cadre de cet exposé, j'en ai extrait les recommandations générales que devrait respecter tout État moderne.

**M. Verschuere.** – Ma question n'est pas agressive. Je la pose parce qu'elle est au cœur de mon propos. Le rapport n'est pas très volumineux. D'après ce document, de nombreuses initiatives doivent être prises. On le savait déjà, cela figurait dans les recommandations de l'OCDE. Les participants à la plate-forme

ont repris des questions qui avaient déjà été posées. On devrait pouvoir discuter ici du rapport confidentiel pour mieux cerner le véritable enjeu. Si les normes ISO sont essentielles, les critères d'attribution de ces normes doivent être discutés dans un débat démocratique. Les critères de sécurité font partie de la loi sur la Banque Carrefour, ils doivent être débattus publiquement. Quand les « experts en sécurité de l'information » seront désignés, qui et que vont-ils protéger ? D'autres normes ISO font référence à la sécurité du système, mais plus aux critères démocratiques. S'il faut poursuivre la rédaction de ces rapports, il est regrettable qu'ils restent secrets et qu'on ne puisse en débattre. Que vont faire les gestionnaires des systèmes informatiques ? Vont-ils attendre la nomination d'un responsable en sécurité de l'information ou vont-ils tenter de maîtriser l'outil en attendant ? Un nouveau rapport secret ne donnera pas beaucoup de résultats.

Je voudrais ajouter une précision importante. Il faut rompre avec la culture du silo, ai-je entendu. C'est vrai et faux à la fois. À mon sens, il faut déplacer les limites du silo. Le SPF Économie, ex-INS, dispose d'informations à caractère personnel, recueillies dans des enquêtes et enregistrées dans sa banque de données. Cet organisme peut communiquer ces renseignements, sur autorisation du Comité de surveillance statistique créé au sein de la Commission de la vie privée, à tous les services publics fédéraux, aux organismes d'intérêt public soumis à l'autorité ou au pouvoir de contrôle ou de tutelle de l'État, à l'exclusion des administrations fiscales. Il faut absolument maintenir des silos ; c'est une question d'enjeu et de maîtrise. Toutes les informations recueillies dans des enquêtes statistiques ne peuvent jamais être révélées dans les cas visés par l'article 29 du Code d'instruction criminelle ni en cas de témoignage en justice. C'est une protection énorme, il faut la maintenir.

Il ne faut pas rompre avec la logique des silos, il faut savoir où placer les limites, savoir qui protéger et de quoi.

\* \* \*

**M. Dechamps, modérateur.** – La parole est à M. Thierry Mansvelt.

**M. Mansvelt.** – Je suis expert en informatique auprès des tribunaux. Vous avez fait allusion au coût économique de notre démocratie. Ce coût, qui

n'est pas uniquement financier, n'est pas réellement pris en compte. Je prends l'exemple de la Commission de la vie privée créée par la loi de 1992. Aujourd'hui, seize ans plus tard, les comités sectoriels ne sont pas encore tous créés : il manque toujours le service des statistiques.

Autre exemple, le Comité R chargé du contrôle des services de sécurité, n'a pas de cellule interne permettant de contrôler les actes des services techniques. À quoi cela sert-il de prévoir des officiers et des contrôleurs si les moyens font défaut ? Il faut savoir quelle politique l'on veut adopter.

**M. Verschuere.** – Le comité sectoriel de statistiques a été créé par une loi de 2006. En attendant, les missions de régulation et de contrôle confiées par la loi à ce comité de surveillance sont exercées par la Commission de la vie privée. Attention, la Commission de la vie privée ne règlera pas tout ; cet organisme ouvre les débats mais ne règle pas les questions.

**M. Mansvelt.** – Si ce comité de statistique est tout à fait récent, il a tout de même fallu plus de cinq ans pour constituer les autres comités sectoriels, parce que les gouvernements successifs ne sont pas arrivés à se mettre d'accord.

**M. Dechamps, modérateur.** – La parole est à M. Poulet.

**M. Poulet.** – Je partage la réflexion du précédent orateur sur la lenteur de la création des comités sectoriels et leur nomination politique. Je tiens à appuyer la remarque du vice-président de la Commission de la protection de la vie privée. On a tendance, dans ce pays, à multiplier les lieux de décision et de sous-décision, en particulier en matière de protection de la vie privée. On a dilué le contrôle de la protection de la vie privée dans divers comités sectoriels qui prennent tous des décisions mais qui sont relativement peu visibles. Le fonctionnement de la Commission de protection de la vie privée est d'ailleurs aussi parfois opaque.

Cette multiplication de comités sectoriels engendre plusieurs problèmes. D'une part, ils sont trop proches des administrations à gouverner ; d'autre part, cela risque de créer des lieux de pouvoir sans réelle cohérence dans la décision.

M. Verschuere a insisté, avec raison, sur le débat démocratique. Proportionnalité et transparence sont de beaux mots mais il faut les confronter à

une véritable réflexion, et pas simplement dans un comité sectoriel que personne n'identifie, que personne ne connaît, qui prend des décisions relativement obscures ; même si elles sont publiées, il n'est pas toujours facile d'y avoir accès ou de les comprendre.

La première automatisation des droits permet à l'administration, indépendamment d'une demande particulière d'un citoyen, de lui rendre le bénéfice d'un droit. C'est extrêmement intéressant d'un point de vue démagogique : il n'y a plus de démarche à entreprendre, le droit est automatiquement conféré et exécuté.. Ma première expérience à cet égard est celle des communes qui octroyaient des mesures de réduction sur la fiscalité communale aux VIPO, parfois légères d'ailleurs. Pour cette raison, elles demandaient au comité de surveillance de la banque carrefour de sécurité sociale une autorisation d'obtenir la liste des VIPO. La BCSS procédait à des vérifications et envoyait aux communes la liste complète des VIPO.

Cette manière de garantir l'exercice d'un droit constitue une façon de procéder. Toutefois, une réflexion un peu plus ouverte et plus démocratique au sein des communes aurait peut-être conduit à d'autres solutions, notamment pour les délibérations communales. La seule décision avait été d'octroyer aux VIPO un avantage fiscal. À partir de là, il a été décidé d'automatiser cet avantage pour qu'ils n'aient plus à le demander. On aurait pu imaginer que ce règlement communal fasse l'objet d'une réflexion pour trouver un autre moyen, moins attentatoire à la protection de la vie privée, par exemple en informant de ce droit tous les contribuables de la commune. De cette façon, on leur rend la maîtrise de la démarche.

Par ailleurs, j'ai eu connaissance que, dans certaines communes, ces transferts d'informations concernant les VIPO avaient très vite été utilisés à d'autres fins, et en particulier pour du *marketing* politique. Il faut être extrêmement attentif. Un débat serait certainement nécessaire.

Nous avons fait un choix pour une administration considérée comme un « *benevolent government* », c'est-à-dire un gouvernement qui prend en charge de manière active les intérêts des citoyens et favorisera la possibilité pour ces citoyens de bénéficier de leurs droits.

D'autres démarches existent. Les Norvégiens ou les Français préfèrent accorder aux citoyens, grâce à ce qu'on appelle le « dossier électronique » citoyen, l'ensemble des informations relatives à leurs données fiscales et de

sécurité sociale. Ceux qui doivent entreprendre une démarche administrative nécessitant l'accès à ces informations, plutôt que de devoir aller les chercher auprès des différentes administrations, peuvent en disposer eux-mêmes et les transmettre directement au service qui les demande.

Ainsi, il existe d'autres modèles. L'important c'est la délibération démocratique éclairée qui doit précéder le choix du modèle. Je me souviens très bien du débat en commission pour la protection de la vie privée au moment de l'introduction de la carte SIS. La seule chose qu'avaient demandée le rapporteur et la Commission était d'avoir un débat démocratique au parlement. Il n'a jamais eu lieu. Il est clair que la carte SIS rend de merveilleux services. Le parlement aurait sans doute suivi cette voie, mais il aurait au moins dû y avoir une appropriation par la population grâce à un débat public.

**M. Dechamps, modérateur.** – M. Quintin devant nous quitter, quelqu'un souhaite-t-il lui adresser une question ? La parole est à M. Verschuere.

**M. Verschuere.** – J'aimerais rebondir sur les deux dernières interventions à propos de l'automatisation des droits. Le principe des silos doit faire partie du débat : comment les créez-vous en fonction des enjeux ? La question des critères, pour la BCSS, fait partie du débat. Toutes les normes ISO ne sont pas structurées de la même manière, et cela en fait également partie. Quels critères de sécurité mettez-vous en avant ?

L'automatisation des droits n'est pas non plus une question théorique. Je ne pense pas tout à fait comme M. Pouillet que ce soit une question de modèle. Quand une personne dispose d'un droit automatique pour une diminution de sa facture d'électricité parce qu'elle a un niveau de revenu inférieur à un plafond fixé, ce n'est pas la même chose que l'exemple que j'ai cité, où l'administration flamande n'accède aux données d'un individu que lorsque celui-ci veut faire usage d'un droit particulier. Si un citoyen demande une bourse d'études, ce n'est pas la même chose que s'il ne la demande pas. Celui qui a un revenu inférieur au plafond fixé et qui a droit à une réduction de sa facture d'électricité, y a droit de toute façon. Le droit est institué. Dans le cas du demandeur de la bourse, le droit n'existe que si la personne l'exerce.

La question de l'automatisation des droits doit être posée service par service, droit par droit, disponibilité par disponibilité. Il faut chaque fois se demander si c'est bien ou non, si on les concentre ou non. Si nous ne nous

posons pas ces questions, nous arriverons – et je ne crains pas de le dire – à des monstres.

Toujours dans cette excellente revue, je lis ces paroles du responsable de l'Union des villes et des communes flamandes: « Les autorités compétentes n'ont pas édité de directives en matière de protection de la vie privée. La législation fédérale s'applique mais elle est à ce point stricte qu'elle mettrait en péril le bon fonctionnement d'une administration communale ». Il décrit également, sans se demander ce qu'on veut en faire, le projet gantois Masterdata : « L'ensemble des données dont doit pouvoir disposer l'administration communale est stocké dans des bases de données centrales, puis actualisées et contrôlées en permanence quant à leur disponibilité, leur fiabilité et leur sécurité. Elles sont intégrées dans une base unique ». Ce n'est pas le système que vous avez décrit. Avec cela, on peut ou non automatiser le droit, mais on n'a débattu de rien.

Il ne faut pas se braquer sur un modèle, mais bien sur le service et la protection des personnes.

**M. Quintin.** – Je suis d'accord avec vous. Il faut raisonner tout en nuance. Le secteur social étant un secteur allocatif, les questions ne se posent pas dans les mêmes termes que pour l'automatisation des droits fiscaux. Il existe une tendance politique affirmant que les pauvres doivent être aidés d'initiative alors qu'une autre, plus libérale, argue que si la personne ne fait pas de demande, c'est son problème.

Un débat a lieu dans les communes concernant l'octroi aux VIPO d'une réduction de taxes sur les immondices ou déchets verts. Nous avons imposé que le règlement communal définisse clairement les catégories à exempter : veufs ou veuves, invalides, orphelins, statut Omnium ou chômeur de longue durée. Nous avons imposé une seconde règle : les communes doivent nous transmettre le fichier des personnes contribuables et c'est sur cette seule base que nous répondons à leurs questions concernant leur statut social ouvrant à des réductions de taxes. Le débat se situe là et non pas au niveau de la Banque Carrefour. Organise-t-on un octroi automatique dans les règlements communaux, fédéraux, régionaux ou communautaires ou laisse-t-on le citoyen le demander ? Ce débat est difficile dans le secteur social car certaines situations frôlent l'absurde. Ce serait le cas pour une personne handicapée à qui l'on imposerait une démarche à la commune et qui devrait écrire une lettre pour bénéficier de dix euros de réduction d'impôt par an !

**M. Verschuere.** – Vos idées sont excellentes et il est bien de les diffuser là où vous le faites. Les règles que vous imposez aux communes sont magnifiques. Les données des CPAS sont plus sécurisées que celles des communes dans les rapports qu'ils entretiennent avec vous. Nous devons réellement débattre de ces questions et non pas affirmer simplement que cela relève de l'efficacité du service ou que ce sont des choix imposés par la technique. Si les possibilités techniques existent, il y a derrière elles un choix qui est primordial et qui est politique. Quant à l'automatisation des droits, elle peut être bonne. J'ajouterai que si certains ne peuvent, par exemple, payer leur électricité, mieux vaut, me semble-t-il, baisser alors le tarif pour tous plutôt que de lutter pour des exemptions. La responsabilité est d'ordre politique et ne doit pas retomber sur celui qui organise le système et qui en déploie toutes les possibilités sans contrôle.

**M. Dechamps, modérateur.** – Je vous invite à rejoindre le foyer pour la pause-café. Nous avons prévu en fin d'après-midi une autre séquence questions-réponses. Je vous informe également que M. Istasse ne pourra malheureusement pas nous rejoindre aujourd'hui, retenu par des impératifs inhérents à la présidence de l'Assemblée.

Je vous propose de suspendre la séance durant 15 minutes. Les travaux sont suspendus.

– *Les travaux sont suspendus à 11 h et reprennent à 11 h 30.*

**M. Dechamps, modérateur, Rédacteur en chef de Citizen<sup>e</sup>** – La parole est à M. Cornet, Commissaire-adjoint en charge de la simplification administrative et e-gouvernement en Région wallonne (EASI-WAL).

## 5. La politique de sécurité de la Région wallonne

### ■ M. Cornet, *Commissaire-adjoint en charge de la simplification administrative et e-gouvernement en Région wallonne (EASI-WAL)*

– Je serai pragmatique et plus euphorique, pour reprendre les termes de M. Huet, dans ma vision de la sécurité. Selon moi, on a toujours les moyens de faire ce que l'on a envie de réaliser.

Je parlerai tout d'abord de l'*e-gouvernement*. Le commissariat à la simplification administrative a pour mission de permettre la suppression des silos lorsque c'est autorisé et de rendre l'administration efficace, conformément aux souhaits des citoyens, entreprises, politiques et autres. Je suis conscient que l'administration doit respecter la vie privée. Le débat politique a eu lieu puisque chaque Région et chaque communauté comprend une cellule à la simplification administrative et à l'*e-gouvernement*.

Le principe de l'*e-gouvernement* est le guichet unique. Le but est d'améliorer le service et de permettre une communication directe avec l'administration. Le citoyen n'aura plus qu'un seul point de contact et ne se perdra plus dans les dédales de l'administration. Il y a évidemment un interface uniforme. Si les routes arboraient des panneaux de circulation différents, on aurait du mal à circuler.

C'est évidemment une révolution dans l'administration. Celle-ci est accessible en ligne partout et à toute heure. C'est la différence avec les horaires stricts des administrations.

Il y a aussi des avantages pour l'administration. Ainsi, on procède à une collecte unique de données et il peut y avoir un retour automatique dans les deux sens. L'administration ne doit pas interroger les usagers à plusieurs reprises.

Quel est le lien avec la sécurité ? Derrière l'e-gouvernement, il y a un facteur de succès, à savoir un traitement correct de l'information relative à l'utilisateur dans le respect du cadre légal et réglementaire. Cela traduit la volonté, malgré le cadre légal, d'être le bon élève, d'éviter d'abuser des données. Il faut évidemment assurer la simplification de ces collectes. Il y a un échange de données des sources authentiques vers l'administration et vice versa. Il y a la fiabilité, la résilience et la disponibilité des données. Ainsi, le cadre légal et réglementaire de même que la sécurité de l'information nous mènent progressivement vers une politique de sécurité.

Les objectifs de celle-ci sont de protéger l'administration contre les risques juridiques, c'est-à-dire d'éviter les abus et de sécuriser tous les systèmes.

C'est aussi de protéger le citoyen contre la violation des données sur la vie privée, de protéger le citoyen et l'entreprise contre la divulgation de données qui n'étaient pas destinées à être rendues publiques. C'est d'assurer la continuité du service. Et pour ce faire, un cadre réglementaire plus global est prévu.

Nous avons défini trois niveaux de sécurité.

Niveau 0 : engagement. Nous avons demandé aux administrations un document faîtier qui détermine leur stratégie, qui définit leurs objectifs et leurs responsabilités. C'est ce que nous appelons le niveau politique.

Niveau 1 : politique de sécurité. On entre ici beaucoup plus dans les détails en précisant comment sera assurée la sécurité, quelles seront les grandes tendances, les grands objectifs à respecter et les grands cadres dans lesquels elle doit s'inscrire. Ce niveau est indépendant de la technologie. Il tient compte des normes minimales BCSS, du questionnaire d'évaluation du registre national et de la loi sur la vie privée. C'est ce que nous appelons le niveau tactique.

Niveau 2 : procédures et recommandations. Il s'agit de mesures hautement techniques (pare-feux, mots de passe...) qui permettent de protéger

les citoyens contre les abus éventuels de la part des fonctionnaires. C'est le niveau opérationnel.

Je reviens au niveau 0. Le gouvernement wallon a créé, par sa note du 14 février 2006, le Service central de sécurité de l'information (SCSI) et le Groupe de travail de la sécurité de l'information (GTSI).

Cette note précise également le rôle du commissariat Easi-Wal. Au niveau des sources authentiques, Easi-Wal est l'accès unique pour toutes les administrations de la Région wallonne, excepté celles qui dépendent directement de la Banque Carrefour de la Sécurité Sociale (BCSS). Easi-Wal représente la Région wallonne pour les contacts avec les sources authentiques fédérales et autres, il assume un rôle central pour les échanges et il organise l'accès à ses données authentiques. Cet accès doit être organisé, sécurisé, tracé, disponible, fiabilisé.

Le SCSI est composé de deux agents du commissariat, ce qui correspond à un équivalent temps plein. Vis-à-vis de la Région wallonne, le SCSI a un rôle de conseil, d'avis et de promotion de politique de sécurité, de cohérence des solutions de sécurité. Il a un rôle de stimulation, de formation et de documentation. Ce dernier rôle est externe au commissariat. En interne, il a l'obligation de créer une politique de sécurité, il gère les projets et met des méthodologies en place, il remplit des tâches opérationnelles internes. Il préside également le GTSI.

Le GTSI se compose de tous les officiers de sécurité des administrations de la Région wallonne. Le rôle de ce groupe de travail est d'introduire et de maintenir une culture de la sécurité dont on s'est en effet aperçu qu'elle faisait assez souvent défaut. Ce n'est qu'au moment où l'on s'est aperçu de la nécessité de disposer des données de la Banque Carrefour de la sécurité sociale ou des entreprises, que l'on s'est rendu compte de l'importance de la politique de sécurité. Il s'agit de transmettre ce principe, ce conseil de sécurité en Région wallonne dans toutes les administrations qui, pour beaucoup, vivent en silos.

Il y a lieu aussi de mettre en place un contexte organisationnel technique et juridique de la sécurité, de définir les lignes directrices des politiques de sécurité en Région wallonne, de définir des normes minimales inspirées de la Banque Carrefour de la sécurité sociale pour la protection de la vie privée, de transposer les normes fédérales et les normes minimales communes entre les administrations wallonnes afin d'améliorer le dialogue entre les administrations.

Le GTSI émet également des avis sur la sécurité et les fait valider par l'autorité adéquate, le gouvernement, l'administration ou un directeur général. Le rôle principal de ce groupe de travail sur la sécurité est de rassurer les personnes qui travaillent dans le domaine de la sécurité informatique et de la sécurité des systèmes d'information, en les groupant, en échangeant des bonnes pratiques, en discutant ensemble des expériences, bonnes ou mauvaises, des procédures mises en place, de la sécurité imposée aux agents.

Aujourd'hui, les officiers de sécurité sont perdus dans leur administration. Souvent un pour quatre cents, ils se trouvent en minorité. Leur rôle semble peu important car ils ne se sentent pas soutenus. En les groupant, on a voulu leur transmettre le message que la sécurité était un sujet important, qu'ils bénéficiaient d'une plate-forme de discussion et de la possibilité d'adresser des propositions au gouvernement de manière à ce que leur rôle soit reconnu et suivi dans leur administration.

J'évoquerai à présent le rôle du SCSI, du GTSI et des administrations. Ces trois grands groupes sont inspirés des notes du gouvernement wallon, de la loi sur la vie privée et des normes minimales de la BCSS. Ces lois nous encadrent et nous permettent d'être de bons élèves de la sécurité de l'information et du respect de la vie privée.

En conclusion, je voudrais conscientiser les personnes, principalement les fonctionnaires généraux responsables des administrations, de l'importance de leur rôle dans le domaine de la sécurité. On a trop souvent le sentiment que la sécurité de l'information relève du conseiller en sécurité. C'est le cas en termes de plans, de politiques, mais les risques qu'implique la politique de sécurité ne relèvent pas de l'officier de sécurité. Il a assumé son rôle en réalisant des audits, en prévenant le fonctionnaire général ou l'administrateur délégué. C'est à l'administrateur général qu'il revient de prendre les décisions en matière de sécurité. Aujourd'hui, ce rôle est trop souvent négligé étant donné que sa mission première n'est pas de veiller à la sécurité, mais il doit pouvoir s'appuyer sur un conseiller en sécurité efficace, pertinent et bien formé. Le rôle de ce conseiller en sécurité n'est pas encore assez reconnu. C'est le message que je veux adresser aux fonctionnaires dirigeants.

\* \* \*

**M. Dechamps, modérateur.** – J’aimerais savoir concrètement comment cela se passe en Région wallonne. Qu’observez-vous ? Si j’ai bien compris, vous donnez des lignes directrices qui doivent, ensuite, être appliquées.

**M. Cornet.** – Ce que l’on observe, c’est une volonté des personnes concernées par la sécurité de se réunir et de partager les informations. Elles souhaitent avoir un *e-gouvernement* intégré, mais éprouvent des difficultés à cet égard. Je pense à l’accès aux Banques Carrefours et aux données inhérentes à la vie privée. Elles ont envie de partager ces expériences et de savoir comment accéder plus facilement, mais légalement, aux données. Elles se posent de nombreuses questions à ce sujet. Se réunir les rassure et leur permet de progresser plus rapidement dans l’offre de services au citoyen. Il s’agit de réunions trimestrielles, de contacts plus réguliers, de demandes d’avis, de coups de téléphone, de contacts directs avec la Banque Carrefour et avec la Commission de la vie privée... Ce réseau se met en place et son importance permet une plus grande efficacité.

**M. Dechamps, modérateur.** – Y a-t-il des mesures concrètes pour résoudre le problème des compétences nécessaires mais non encore acquises ?

**M. Cornet.** – Lors de la première réunion du groupe de travail consacré à la sécurité, le premier souci des officiers de sécurité a été de demander une formation. Des formations sont données dans différentes facultés universitaires mais il n’est pas toujours évident pour une personne affectée à la sécurité pour un dixième de son temps de travail de pouvoir suivre une pareille formation.

Nous allons donc essayer de mettre au point des formations qui existent peut-être ailleurs – dans les facultés universitaires ou à la Banque Carrefour de la sécurité sociale – mais pas à l’échelon wallon et qui ne sont pas toujours suffisamment pragmatiques.

**M. Dechamp, modérateur.** – Y a-t-il encore une question pour M. Cornet ?

**Une intervenante.** – Je voudrais savoir comment l’échange de l’information est organisé à l’échelon régional. On a vu qu’à la Banque Carrefour les échanges sont sécurisés.

**M. Cornet.** – Je vais vous dire comment nous voudrions que cela se passe. Nous voudrions suivre le modèle de la Banque Carrefour. Le

Commissariat aurait un rôle central pour interroger les banques carrefours autres que régionales. Nous souhaiterions jouer ce rôle central et permettre aux administrations d'aller chercher les données là où elles sont. Ce qui n'est pas tout à fait le cas à l'heure actuelle. Notre objectif est donc de créer une sorte de « Banque Carrefour wallonne » afin de gagner en efficacité.

Voilà le modèle vers lequel nous voulons évoluer. La décision du gouvernement a été claire et les administrations sont en train de nous suivre dans cette voie.

**M. Dechamps, modérateur.** – Y a-t-il encore une question ?

**Une intervenante.** – Je voudrais poser deux questions. Tout d'abord, M. Cornet a parlé des officiers de sécurité wallons. J'aimerais simplement savoir quel sera leur rôle. Ce débat est fondamental pour la protection des données. Quel est leur impact sur leur administration dans la surveillance et l'utilisation des outils, l'accès et les autorisations accordées ?

Je voulais savoir aussi si Easi-Wal est le point de contact pour organiser les accès et les autorisations vers les services fédéraux et régionaux mais pas vers les pouvoirs locaux.

**M. Cornet.** – C'est ça.

Votre première question est plus vaste. Je vais essayer de définir le rôle de l'officier de sécurité avec exactitude. Il consiste pour l'instant à prévenir la hiérarchie des risques existants avec les systèmes de sécurité installés afin qu'elle puisse prendre les bonnes décisions. Elle doit en effet en quelque sorte accepter ce risque mais aussi l'évaluer par rapport aux cadres légaux. En plus de conseiller le sommet de leur hiérarchie et le gouvernement, les officiers de sécurité ont aussi un rôle opérationnel dans le sens où ils doivent créer les politiques de sécurité. Le prochain groupe de travail va justement plancher sur la fonction des officiers de sécurité en Région wallonne.

**M. Verschuere.** – J'aimerais faire une remarque. La loi sur la « vie privée », dans son article 17bis, dit que le Roi peut déterminer que le responsable du traitement désigne un préposé indépendant à la protection des données. Dans un arrêté du gouvernement, la Région pourrait aussi lui donner une garantie d'indépendance. Dans les règles fédérales, le Roi détermine son statut, ce qui est indispensable pour assurer son indépendance. À un moment

donné le système doit arriver à en faire un référent indépendant. Il faut garantir sa liberté d'action pour que sa mission ait du sens.

**M. Dechamps, modérateur.** – Nous aurons l'occasion de continuer le débat, soit après votre exposé, soit en fin d'après-midi.

**M. Dechamps, modérateur,** Rédacteur en chef de Citizen<sup>e</sup> – La parole est à M. Martin, Conseiller en Procédure et Sécurité, Entreprise publique des Technologies Nouvelles de l'Information et de la Communication de la Communauté française (ETNIC) pour l'Etnic et M. Delaunoy, Conseiller en Sécurité au Ministère de la Communauté française pour la Communauté française.



## 6. Analyse des risques à la Communauté française

### ■ M. Martin, Conseiller en Procédure et Sécurité, Entreprise publique des Technologies Nouvelles de l'Information et de la Communication de la Communauté française (ETNIC)

– Nous sommes venus à deux, Pierre Delaunoy et moi, pour respecter ce qui se passe sur le terrain. En effet, c'est à deux que nous procédons aux analyses de risques. C'est aussi une bonne manière d'illustrer qu'il n'y a pas d'analyse de risques sans une excellente collaboration entre le fonctionnel que représente Pierre Delaunoy et le technique que je représente.

Tout à l'heure M. Pouillet demandait à la Communauté française de fournir un gros effort pour protéger les données du citoyen. Nous partageons cette demande qui rejoint nos préoccupations. L'analyse des risques que nous allons vous présenter est une illustration de nos efforts dans ce sens.

Au cours des formations organisées par les Facultés universitaires de Namur et par l'ICHEC, pour les conseillers en sécurité de l'information j'ai eu l'occasion de côtoyer des confrères venant d'autres organismes privés et publics. J'ai ainsi appris que si je me décourageais parfois devant l'ampleur du chemin qui reste à parcourir je n'étais pas le seul dans le cas, et que sur certains points nous pouvions supporter avantageusement la comparaison..

L'analyse des risques à la Communauté française a débuté il y a environ deux ans. À l'époque, M. Huet du Service public fédéral des technologies de l'information et de la communication (Fedict) nous avait expliqué lors d'une séance de travail commune que la méthode *Quick-Win* d'analyse des risques était intéressante et qu'elle pouvait être mise en œuvre avec très peu de moyens financiers. Des agents de l'Étnic et de la Communauté française ont donc suivi la formation proposée par le fedict et la méthode que nous utilisons aujourd'hui en est très proche.

Notre démarche d'analyse des risques poursuivait trois objectifs. Le premier était d'évaluer les risques liés aux processus. Le deuxième était d'en dégager une série d'exigences pour les ressources humaines, informatiques et autres. Le troisième était d'en tirer une liste d'éléments susceptibles d'être améliorés.

De ces trois objectifs principaux en découlent deux autres que l'on peut qualifier d'intermédiaires. D'une part, nous prenons connaissance des principales menaces pesant sur ce processus, et, d'autre part, on s'interroge sur l'impact qu'aurait un incident.

Ce qui est très intéressant dans la méthode *Quick-Win*, c'est qu'elle s'intéresse aux impacts possibles aux niveaux de tous les intéressés à savoir : les citoyens, les agents de la Communauté française et ceux de l'Étnic.

Grâce à l'utilisation d'une méthode bien définie, on peut reproduire, avec des interlocuteurs différents un exercice qui donne des résultats comparables. Nous verrons dans les conclusions que cela a aussi été fort apprécié par nos interlocuteurs qui voyaient dans cette méthode une manière de structurer le raisonnement qu'ils avaient déjà entamé dans le cadre d'une bonne gouvernance. Cette méthode leur apporte un fil rouge et leur permet de progresser.

Je voudrais rappeler ici en quelques mots , en guise de support à la suite de l'exposé, les concepts de base de la sécurité.

On considère qu'il y a un risque sur un processus lorsqu'il y a une probabilité d'impact négatif suite à un dysfonctionnement ou à un incident.

Pour qu'il y ait probabilité d'incident négatif il faut qu'il y ait à la fois des menaces et des vulnérabilités. Un exemple : un ordinateur qui n'aurait

qu'un seul utilisateur, particulièrement prudent et qui n'utiliserait que des logiciels sûrs, court très peu de risques. Par contre, le risque augmente si on utilise des logiciels plus « exotiques » avec des utilisateurs plus « créatifs ». La probabilité d'incident dépend de l'importance des menaces, de l'attractivité des fraudes possibles et des failles dans les protections, c'est-à-dire les vulnérabilités. Nous reparlerons de tout cela au moment de faire l'analyse.

Dernier principe : un processus est exposé à l'ensemble des risques pesant sur ses différents constituants. Comme je l'ai dit, il y a des constituants humains et informatiques. C'est à l'ensemble de ces risques qu'est exposé le processus.

Nous ne nous attarderons pas sur la formule mathématique qui se veut scientifique dans un domaine qui l'est très peu. Il en découle que le risque sur la totalité est la somme des risques sur les différents éléments.

Le point suivant concerne une légère adaptation de la méthode *Quick-Win*. Nous commençons d'emblée par interroger le responsable du processus sur les impacts qu'auraient une non-disponibilité du processus, un manque d'intégrité au niveau des données ou une perte de confidentialité. Cela constitue notre point de départ qui s'assimile à l'étude de contexte qui est la première étape dans la plupart des méthodes d'analyse des risques. Nous avons en effet remarqué que ces personnes, sans disposer de méthode particulière, avaient conscience de ce qui les menaçait et de ce qui pouvait les protéger. Il est inutile de se priver de cette réflexion préalable, que nous appelons « phase globale d'analyse ».

Si cette phase d'globale d'analyse conduit, par exemple, à la conclusion que le processus ne traite que des données publiques, nous pourrons, dans les phases suivantes éviter d'étudier les risques liés à la confidentialité. Cela nous permet de simplifier le processus.

Nous passons ensuite à la phase analytique qui se base sur la même technique d'interview. Cette phase laisse plus de place aux scénarii. Un scénario étant une combinaison de menaces et de vulnérabilités pouvant conduire à des incidents. Nous pouvons constater que nos interlocuteurs possèdent une bonne vision de ces scénarii. Nous ne jouons qu'un rôle de catalyseur en leur faisant réfléchir à des aspects ou des scénarii additionnels auxquels ils n'avaient pas pensé. Nous évitons, en tous cas d'évaluer à leur place.

Les résultats de l'exercice correspondent aux objectifs que nous nous sommes fixés. Nous obtenons en effet une vue sur les risques globaux encourus par le processus tout en découvrant les menaces principales qui les génèrent. Nous découvrons aussi la nature et l'importance des impacts par type d'incident et nous établissons une liste des améliorations qui devraient être mises en œuvre.

**M. Delaunoy**, Conseiller en Sécurité au Ministère de la Communauté française – Je voudrais aborder ici l'analyse de risques du côté pratique.

Quels sont les pré-requis indispensables pour une bonne analyse de risques ? La participation des décideurs à l'analyse constitue l'élément fondamental. Le décideur est un fonctionnaire général, au minimum un directeur général. Les participants doivent être motivés et concentrés car de nombreuses questions sont posées et les réponses sont variées.

Un autre pré-requis est un schéma de circulation de l'information mettant en évidence les sources d'information, les processus du traitement et les consommateurs d'information. Il faut aussi beaucoup de patience, dans le chef tant des participants que de l'auditeur. Les réponses partent parfois dans tous les sens et il convient souvent de recentrer les débats.

Je citerai un postulat de départ. Nous considérons que les risques de perte de confidentialité, d'intégrité et de disponibilité ainsi que la non-imputabilité sont pris isolément, simplement pour garder les questions les plus simples possible mais aussi pour disposer d'un outil informatique qui ne soit pas trop difficile à manier.

Enfin, tout ceci permet de comparer ultérieurement les analyses de risques entre elles. C'est très intéressant pour les auditeurs qui peuvent ainsi se remettre en question.

Le deuxième point important de la méthode est la métrique. Elle porte sur trois aspects : les pertes financières, les pertes de temps et les pertes d'image. Chaque risque est coté de 0 à 4 : 0 représente l'absence de risque, 1 représente un risque pour les pertes financières allant jusqu'à 2 500 euros, les pertes de temps jusqu'à dix jours par homme et les pertes d'image jusqu'à une perte de qualité perçue par cent personnes. Et ainsi de suite jusqu'au degré quatre pour lequel les dégâts sont supérieurs à 250 000 euros.

J'en viens au choix des ressources. L'analyse de risque se déroule en deux parties : une phase globale et une phase plus analytique. Une ressource

est choisie en fonction des résultats de la phase globale. Elle ne peut bien évidemment pas se limiter à des aspects purement technologiques. Elle doit être un élément significatif du traitement. Par exemple, elle peut être le facteur humain, les membres du personnel, des dossiers papier ou un ensemble de serveurs. Il est parfois surprenant, quand on procède à une analyse de risque, de constater à quel point les agents de l'administration sont surpris que l'on puisse poser des questions sur la confidentialité et l'intégrité de leurs dossiers papier. Bizarrement, cela les préoccupe davantage que l'aspect purement technologique.

La cotation du risque est un point important. Comment évaluer correctement un risque ? Prend-on le cas le plus défavorable ? Par exemple, lorsqu'il s'agit d'un processus de paiement de salaire, doit-on considérer que l'ordinateur pourrait tomber en panne juste le dernier jour, au moment du paiement ? Ou opte-t-on pour une mesure beaucoup plus raisonnable ? En fait, nous avons choisi une adaptation de la loi de Pareto et considérons que le risque est coté dans 80 % des circonstances les plus défavorables. Les autres 20 %, les plus catastrophiques, n'interviennent pas dans la cotation. Cela ne signifie pas qu'on les ignore. Un scénario prend en charge ce genre de cas. Si on souhaite conserver le principe du postulat de départ, à savoir l'isolation des risques, on préfère coter un risque dans 80 % des cas.

Je citerai enfin quelques bonnes pratiques. Il est très facile de glisser un chiffre à un groupe pour que celui-ci l'avalise. Il est donc préférable que l'auditeur n'influence pas les réponses des participants. En cours d'interview, il faut toujours procéder à un petit calcul rapide pour disposer d'une moyenne des risques liés aux ressources et la comparer au niveau global. Cela permet de se faire une idée de la cohérence des réponses fournies par les participants. Enfin, il faut prendre le temps d'étudier les résultats avant de venir aux conclusions, celles-ci étant, dans ce cas, des mesures supplémentaires de sécurité.

Pour la conclusion, je passe la parole à M. Martin.

**M. Martin.** – La première conclusion est que les choses se sont passées beaucoup mieux que prévu. Un des bénéfices additionnels d'une méthode relativement simple et prenant peu de temps est que l'on peut s'adresser à des interlocuteurs au niveau adéquat. Ces interlocuteurs ont déjà des préoccupations relatives à la sécurité de leurs opérations et ce que nous leur apportons est l'occasion de réunir leur staff pour mener avec méthode une réflexion qu'ils souhaitent.. C'est tout bénéfique pour nos interlocuteurs mais ce

l'est aussi pour nous, puisqu'en tant que conseillers en sécurité, nous ne pouvons déterminer les mesures de sécurité transversales les plus adéquates qu'au travers des connaissances acquises au travers de ces exercices.

M. Cornet, tout à l'heure, nous a parlé de la politique de sécurité en Région Wallonne. Il existe une très grande complémentarité entre la politique de sécurité et l'exercice d'analyse des risques. Je ne vous surprendrai en effet probablement pas beaucoup en vous disant que le texte de la politique de sécurité n'est pas considéré par les différentes hiérarchies des Organismes de la Communauté française comme un document « passionnant à lire absolument ». Mais une fois que l'on a effectué l'analyse des risques, ce document est perçu différemment. Il apparaît alors comme un début de réponse, une voie à suivre pour contenir les risques découverts.

Le fait de procéder à cette analyse avec le staff et les responsables des différents services contribue énormément à diffuser dans les différentes entités de la Communauté française une « Culture de la sécurité ».

Notre dernier transparent est relatif à l'évolution de la méthode. Jusqu'ici nous l'avons appliquée à des périmètres bien spécifiques. A l'avenir les deux dimensions supplémentaires consisteront à tirer des leçons transversales des différents besoins et à analyser pour chaque périmètre l'évolution des risques dans le temps. L'objectif final étant non pas d'analyser mais bien d'améliorer.

\* \* \*

**M. Dechamps, modérateur.** – Je propose de passer aux questions relatives à l'analyse des risques.

**M. Pouillet .** – Depuis que vous appliquez cette méthode, quels risques ont été révélés ?

**M. Martin.** – Dans la majorité des processus administratifs étudiés ce sont davantage des risques de perte de confidentialité et d'intégrité qui ont été découverts plutôt que des risques liés à l'indisponibilité du processus ou des

ressources. Comme Pierre Delaunoy le disait tout à l'heure, le plus marquant est la réaction des participants à la question de savoir ce qui se passerait si leurs dossiers papier disparaissaient. L'administration reste l'administration et je crois que le papier a encore de beaux jours devant lui.

**M. Delaunoy.** – En fait, ce n'est pas tellement la plate-forme technologique qui constitue le principal risque, mais bien la confidentialité tout au long des processus.

**M. Verschuere.** – Vous êtes pour l'instant dans un processus d'analyse des risques avec la perspective de dégager des solutions. En êtes-vous déjà au stade de l'élaboration de solutions ?

**M. Martin.** – Oui nous avons déjà eut l'occasion d'identifier et de lancer la mise en œuvre de solutions simples et peu coûteuse pour rencontrer certains risques. On s'est aperçu, par exemple, que dans une application on devait donner l'accès au numéro du registre national à certains utilisateurs mais que cet accès était par défaut accordé même aux utilisateurs qui n'en avaient pas le besoin.. La modification à apporter au logiciel n'était pas difficile à implémenter.. Des solutions simples et peu coûteuse sont donc parfois faciles à dégager.

**M. Verschuere.** – Qu'en est-il de l'accès à ce numéro et de la gestion des fichiers via ce numéro ?

**M. Martin.** – On n'a pas la sensation d'avoir atteint l'objectif.

**M. Verschuere.** – Il vaut mieux y penser que fermer les yeux.

Lorsque vous soumettrez le résultat de votre analyse à votre hiérarchie, comptez-vous lui dire que vous avez déjà envisagé des solutions possibles, ainsi que leur planification, et lui faire part de votre incapacité à les mettre en œuvre au stade actuel pour des raisons financières, humaines ou de culture d'entreprise ? La culture d'entreprise, c'est parfois le simple fait d'avoir des bureaux ouverts plutôt que des bureaux fermés et de faire passer tout le monde devant le même matériel.

**M. Martin.** – La culture d'entreprise a été pour nous une très bonne surprise. Nous pensions que nous serions taxés « d'œil de Moscou » ou d'empêcheurs de tourner en rond, mais ce ne fut pas le cas. Le problème ne

réside pas là, le problème, c'est que les bonnes résolutions s'estompent rapidement. On sait qu'il faut agir, mais d'autres questions plus urgentes priment.

Les petites choses sont faciles à mettre en oeuvre. Quant aux grandes, on espère les réaliser lorsque l'agenda le permettra.

**M. Verschuere.** – Vous exercez une mission et vous avez un rôle à remplir. À un moment donné, il faut que l'ensemble du système prenne la décision.

**M. Martin.** – Exactement. C'est pourquoi il est utile que la hiérarchie participe aux analyses de risque et au plan de sécurité que nous rédigeons.

**M. Dechamps.** – Comment appliquez-vous la notion de métrique aux citoyens ? Notre débat porte en effet sur la protection des données à caractère personnel. Vous avez évoqué les pertes financières, de temps et d'image, mais tout cela est vu du côté de l'administration. Qu'en est-il du côté du citoyen ?

**M. Martin.** – Les pertes financières, de temps et d'image sont évaluées pour le ministère, l'Étnic, mais aussi les tiers. On essaie d'évaluer les dégâts pour les tiers, par exemple en cas de perte de confidentialité d'un dossier.

**M. Dechamps.** – Mais pas pour le citoyen final ?

**M. Martin.** – Nous essayons.

**M. Dechamps.** – C'est évidemment difficile à évaluer.

**M. Martin.** – Supposons, par exemple, que des fonctionnaires soient payés avec quatre jours de retard. Seule une petite partie d'entre eux en souffrent vraiment et nous cherchons donc à les identifier, en essayant de savoir quelles seraient les conséquences de rappels de banque, etc. Cette évaluation a seulement le mérite d'exister et non de produire un résultat productif.

**M. Dechamps.** – Et en termes de confidentialité ?

**M. Martin.** – C'est plus difficile. Mais Comme on est dans une administration, le fait de contrevenir à la loi est un élément auquel on est sensible bien qu'il soit difficile de mesurer quelle pourrait être les conséquences pour le citoyen d'une perte de confidentialité

**M. Verschuere.** – N'oubliez pas que la Commission de la protection de la vie privée se tient à votre disposition. Voici un exemple qui doit plaider en faveur de la politique que vous menez. La commission a été saisie d'une demande d'avis de la ministre-présidente de la Communauté française qui se demandait si elle pouvait exploiter le fichier des élèves, que possède son administration, pour adresser aux parents des jeunes filles de moins de quinze ans un courrier personnalisé à propos du vaccin contre le cancer du col de l'utérus.

La réponse fut que cela ne posait pas de problème puisqu'il s'agissait d'une politique publique de prévention concernant la santé des élèves. Toutefois, ce qui était très intéressant, c'est que ce dossier comportait des mesures préventives du risque, qui ont balayé toute une série de questions que nous aurions pu nous poser. Le fichier n'a pas été transmis au cabinet, mais ce sont les fonctionnaires en possession du fichier qui ont effectué l'envoi. Il n'y a donc pas eu d'extraction ou de constitution d'un nouveau fichier, mais un simple routage. La description du processus, comportant des évaluations de critères et de protection, était très intéressante.

Même si la Commission de la protection de la vie privée ne doit pas être saisie systématiquement, les administrations ne doivent pas hésiter à le faire lorsqu'elles ont un doute par rapport à une pratique nouvelle ou lorsqu'elles se posent des questions. La loi est faite non pour interdire, mais pour accompagner les processus.

**M. Martin** – Nous allons en abuser !

**M. Verschuere** – Plus vous demanderez, plus les réponses tarderont.

**M. Martin** – Il est vrai qu'il s'agit d'une matière complexe. Et que les objectifs poursuivis sont souvent contradictoires.

**M. Verschuere** – Il s'agit évidemment d'une matière sensible. La ministre ne voulait pas se voir reprocher d'avoir abusé d'un fichier d'élèves et sa démarche préventive, correcte et intéressante, nous a forcés à réfléchir. Il s'agit d'une amorce de dialogue et les réponses sont transposables à des situations semblables.

**M. Martin** – C'est ce que nous faisons.

**M. Verschuere** – Les avis de la Commission de la protection de la vie privée ne sont pas contraignants et nous sommes à l'écoute d'un désaccord

éventuel. J'ai participé, voici quelque temps, à une journée d'étude sur les caméras de surveillance à Namur, à l'invitation d'Yves Poullet. L'un des intervenants a déclaré que la loi sur les caméras de surveillance était scandaleuse, que la Cour de cassation avait rendu un avis à ce propos en 2004, que le Conseil d'État s'était également prononcé en 2003, alors qu'en 1999, la Commission de la protection de la vie privée avait rendu un avis qui n'a pas été respecté ! Nous n'avons pas nécessairement raison.

Il n'est pas certain que nous ayons raison. Dans nos avis, nous soulevons des questions. Ces avis peuvent évoluer au fur et à mesure du débat car des avis péremptoires peuvent être parfois rendus sur la base d'informations parcellaires sur des sujets que l'on ne maîtrise pas. Ils ouvrent alors un débat mais ne constituent pas une vérité à laquelle vous devez vous soumettre. Vous devez nous renvoyer des questions relatives aux sujets qui relèvent de votre compétence et non une réflexion globale. Nous ne transmettons que des avis et la seule obligation de l'administration sera de motiver sa décision si elle ne les suit pas.

**M. Dechamps, modérateur,** s'adressant à M. Verschuer – Une proposition de loi vise à instituer une commission spéciale chargée d'évaluer la politique menée en matière de protection de la vie privée. Cela ne fait-il pas double emploi avec votre fonction ?

**M. Verschuer.** – Non. Il s'agirait d'une assemblée comme celle-ci, mais elle serait permanente. La qualification et les tâches de cette commission spéciale devront être précisées par le parlement. Il est absurde d'évaluer le travail de la Commission de la protection de la vie privée puisqu'il s'agit d'une commission indépendante.

Nous avons eu des contacts avec les auteurs de la proposition. Nous leur avons dit que nous ne voulions pas de la création, au sein du parlement, d'une commission de surveillance, comme c'est le cas pour le comité R ou le comité P. Nous ne devons pas être surveillés puisque ce que nous faisons est public. Nous ne réalisons pas d'enquêtes secrètes sur des policiers masqués qui auraient commis des abus.

Le vrai problème, c'est que notre travail manque d'écho. Nos avis sont publiés sur un site mais s'il n'est pas consulté, cela ne sert à rien. Il est important qu'il y ait, au sein du parlement, une commission spéciale dotée des mêmes pouvoirs qu'une commission permanente et qui peut donc examiner les

propositions et projets de loi, les adopter ou les renvoyer en séance plénière. C'est peut-être un effet de mode mais, si cela favorise le débat, c'est très bien. Cela permettra qu'échappent aux discussions de couloir de fin de nuit lors des accords de gouvernement, des questions essentielles comme le dossier médical, qui se retrouvent inscrites dans un projet sans débat réel, après éventuellement un avis rendu trop rapidement par la commission. Si des politiques sont d'accord sur la forme, mais non sur le fond, un débat public doit avoir lieu mais pas au milieu de la nuit !

Nous souhaitons vraiment que cette commission puisse faire aboutir quelques dossiers et puisse au moins organiser un débat ouvert. Les États-Unis, qui ont une culture assez particulière en matière de protection des personnes, font preuve d'une raideur terrible vis-à-vis de leur administration. Tous les projets administratifs sont soumis à un *privacy assesment* avant que ceux-ci soient financés ou mis en oeuvre. Ce *privacy assesment* est réalisé par l'officier de sécurité de l'administration. L'*assesment* est ensuite soumis pour validation aux *data protection authorities*.

Aux États-Unis, ce processus de pré-autorégulation est très intéressant et très performant pour les administrations publiques.

Les pouvoirs privés, quant à eux, vous surveillent plus que d'autres. Cette commission parlementaire pourrait mener un débat sur ce processus et éventuellement créer une transversalité avec les pouvoirs fédérés. À mon avis, cela donnerait de meilleurs résultats que des plates-formes de coopération à rapports secrets.

**M. Dechamps, modérateur.** – La parole est à M. Jongen.

**M. Jongen.** – Les professionnels de la santé demandent clairement que les politiques surveillent le respect de la loi sur la vie privée, notamment la signature électronique, l'utilisation du registre national, etc. Nous avons l'impression que des décisions se prennent très vite, parfois en l'absence de contrôle. Dès lors, on se retrouve avec des projets thématiques où le secret n'est manifestement pas préservé et contre lesquels il faut alors se battre. Le politique doit certainement exercer un contrôle plus important.

**M. Verschuere.** – Comme je l'ai souvent indiqué, il faut descendre dans la rue. Après ce colloque, chacun rentrera chez soi et il ne se passera pas grand-chose. Or il est possible de saisir cette Commission de la protection de la

vie privée afin de l'obliger à réfléchir. Cette réflexion est essentielle. Il ne faut pas nous demander si l'utilisation du registre national est pertinente ou non dans le cadre du dossier médical informatisé. Le nom est un code, public ou privé, mais la question de la codification n'est pas fondamentale. C'est vous qui devez soulever les questions.

La Commission de la protection de la vie privée met de l'ordre dans le questionnement. C'est une instance d'experts qui éclaire et dresse simplement l'état de la situation. C'est à vous ensuite d'intervenir.

En matière des droits du patient, par exemple, quelle information masque-t-on ? Lorsqu'une personne qui possède un dossier médical informatisé se rend chez son généraliste, elle n'a pas nécessairement envie de dire qu'elle a subi deux avortements ou qu'elle est suivie par un psychiatre pour des assuétudes. A-t-on encore le droit de mentir à son médecin ? Les médecins ont-ils le droit de savoir ce que font leurs confrères ? Où se situe la liberté thérapeutique ? Que transmet-on dans ce dossier ? Les annotations personnelles du médecin s'y trouveront-elles étant donné que les médecins n'auront plus nécessairement de support papier ?

Vous pouvez formaliser toutes ces questions, mieux que nous. Nous pourrions alors en débattre et vous dresser un état le plus pertinent possible de la situation. Plus la démarche et la réflexion seront de qualité, plus le politique sera enfermé dans le cadre que nous aurons créé. Il ne sera pas d'accord avec ce cadre, mais il devra le dire, s'expliquer et poursuivre sa démarche.

C'est ce qui s'est passé avec les caméras de surveillance. Les résultats ne sont peut-être pas très bons mais les choses iront en s'améliorant si nous persistons.

Votre question relative au dossier médical informatisé est essentielle.

Certains médecins font l'apologie de la média-médecine. Grâce à elle, ils pourraient s'occuper davantage des personnes et moins de leur dossier. C'est pourtant difficile à prévoir. Ce sont de toute façon les médecins qui doivent fixer les enjeux.

J'ai beaucoup apprécié le recours introduit devant la Cour d'arbitrage par les médecins contre le décret flamand. La Cour n'a toutefois pas tout annulé. Elle a intelligemment validé de nombreuses dispositions mais a souligné

que certaines autres étaient mal motivées. C'était notamment le cas de la transmission des données et annotations personnelles des médecins. D'autres points n'ont pas davantage fait l'objet d'un débat. Je citerai ainsi la présomption du consentement du patient pour la transmission de ses données. La Cour a finalement annulé deux dispositions mais les médecins ont porté devant cette institution les questions fondamentales qu'ils voulaient défendre. Ils auraient peut-être dû le faire avant. Il faut toutefois poursuivre ce débat. Je vous encourage à le faire.

**M. Dechamps, modérateur.** – Les travaux sont suspendus pour la pause-déjeuner.

– *Les travaux sont suspendus à 12 h 50 et reprennent à 14 heures.*

**M. Dechamps, modérateur,** Rédacteur en chef de Citizen<sup>e</sup> – Pour des raisons d'actualité, nous devons libérer cet hémicycle avant 16 heures. M. Vercruysse, de l'Union des villes et des communes wallonnes ne pouvant nous rejoindre pour des raisons de santé, je donne la parole à Mme Rouma, responsable du Registre national.



# 7. L'organisation de la gestion de l'identité en Belgique

## ■ Mme Rouma, Responsable du Registre national

– Je commencerai par définir la notion d'identité en examinant son évolution dans le temps et la façon dont la Belgique, précurseur dans le domaine, en a organisé la gestion. Je parlerai ensuite de la carte d'identité électronique en tant qu'outil permettant de renforcer la protection de la vie privée. Je vous livrerai enfin quelques pistes de réflexion inspirées d'un livre blanc rédigé en France pour préparer un débat sur l'administration publique.

Étymologiquement, le mot identité signifie une chose et son contraire. *Identitas* désigne des choses semblables ; dans le langage courant et juridique, l'identité désigne cependant le fait pour une personne d'être un individu qui peut être reconnu pour tel, sans aucune confusion possible, grâce à des éléments qui le distinguent, comme l'état civil.

Au Moyen-Âge, le terme « identité » était consacré par le droit canonique. La personne individuelle était établie comme étant un fidèle baptisé.

L'ordonnance de Villers-Cotterêts du 15 août 1539, signée par François 1er, a réellement jeté la première pierre de l'état civil en imposant au curé de paroisse l'obligation de consigner les naissances et les décès dans des registres contresignés par un notaire et déposés au greffe du bailli ou du sénéchal.

J'ai relu cette ordonnance et j'ai relevé ce qui suit : « Ainsi date de majorité et de minorité, preuves de filiation et du décès pouvaient être officiellement établies ». C'est une date très importante qui a jeté les bases de l'état civil et de la reconnaissance de l'identité.

L'identité peut être définie comme la relation entre une personne biologique et un jeu unique de paramètres qui la décrivent : les paramètres biométriques et les paramètres sociétaux. La conception sociétale de l'identité est donc largement utilisée dans le droit civil où l'identité est isomorphe de la filiation.

Dans une société organisée, l'identification correcte des individus doit être un objectif premier des autorités publiques. L'identité est en effet le complément naturel de l'attribution d'une personnalité juridique à une personne. Il s'agit d'une nécessité pour la sécurité physique de toute personne. Elle donne à la personne la possibilité d'exercer ses droits sociaux et politiques, et de faire face à ses obligations légales ou contractuelles. Elle facilite bien entendu les recensements démographiques et les différentes études sur la population réalisées dans des buts économiques ou scientifiques. Elle permet également d'assurer la protection des personnes et des propriétés, le contrôle des flux migratoires et la sauvegarde des intérêts vitaux de l'État.

Dans le monde réel, l'identité est circonscrite par les attributs constitutifs de l'état civil : le nom patronymique, le ou les prénoms, la date et le lieu de naissance, la nationalité et le sexe. On peut donc considérer que l'identité publique originelle et originale unique, stable et permanente est attestée et garantie par l'État. C'est celui-ci qui fixe les règles selon lesquelles sont attribués les éléments constitutifs de l'identité.

Le droit à l'identité est-il un droit de l'homme ? J'ai consulté la Convention européenne et la Déclaration universelle des droits de l'homme. Le droit de disposer d'une identité attestée et protégée par l'État n'y figure pas de manière explicite. Par contre, la Convention internationale des droits de l'enfant stipule en son article 8 que les États parties s'engagent à respecter le droit de l'enfant et à préserver son identité, y compris sa nationalité, son nom et ses relations familiales, tels qu'ils sont reconnus par la loi sans ingérence illégale. Cet article stipule également que, si un enfant est illégalement privé des éléments constitutifs de son identité ou de certains d'entre eux, les États parties doivent lui accorder une assistance et une protection appropriées pour que son identité soit rétablie aussi rapidement que possible. Donc, le droit à l'identité est bien un droit fondamental.

Outre l'identité traditionnelle, le développement des technologies de la communication a engendré la notion d'identité numérique, un concept beaucoup plus vaste, aux contours beaucoup moins clairs que le concept d'identité traditionnelle. Certaines données numériques qui ont trait à l'individu comme les mots de passe, les codes d'accès, les pseudonymes virtuels ne sont, dans la plupart des cas, pas considérées comme constitutives de la personnalité juridique d'une personne.

On constate aujourd'hui que les identifiants numériques font de plus en plus l'objet d'actes malveillants. Ceci amène une perte de confiance dans les nouvelles technologies de l'information et de la communication. De plus en plus d'États interviennent pour sanctionner plus rigoureusement ces comportements frauduleux. L'Europe se préoccupe également de la fraude à l'identité.

L'identité est en effet un des piliers à la libre circulation consacrée par le Traité européen. La prolongation digitale de ce droit à la libre circulation est la libre concurrence dans les réseaux de communication et des services électroniques.

Une conférence sur l'identité et la fraude a été organisée au cours de la présidence portugaise du Conseil. Elle recommande de développer une approche commune. Néanmoins, la définition et le cadre légal de l'identité divergent selon les pays. Cela pose donc un problème. Il a été décidé de réaliser une étude afin de faire le point sur les systèmes nationaux de documents électroniques d'identité. Les résultats pourront servir de supports aux États membres pour qu'ils élaborent des normes d'identification en vue de diminuer les risques de fraude.

Après l'évolution de la notion d'identité, je vais à présent me pencher sur l'organisation de la gestion de l'identité en Belgique. Celle-ci suppose un système rigoureux d'enregistrement de la population. En Belgique, la gestion de l'identité est intimement liée à l'inscription dans les registres de la population fondés sur les actes d'état civil et, de là, au registre national. Ce système est une spécificité belge mise en place dès 1846, après le premier recensement général de la population belge.

La carte d'identité a été introduite en Belgique par l'occupant allemand pendant la première guerre mondiale. Elle a été maintenue et généralisée dès 1919. Elle est considérée comme un certificat d'inscription dans les registres de la population. Elle constitue pour le détenteur la preuve qu'il est titulaire d'une

identité déterminée. Elle permet également de se faire reconnaître comme étant la personne qu'il prétend être dans ses relations avec l'autorité publique mais aussi dans ses relations sociales.

Le passage des registres de population au registre national constitue le passage à l'identité digitale liée à un identifiant unique. Le registre national des personnes physiques reprend les données d'identification et de localisation des personnes inscrites au registre de la population et des Belges immatriculés auprès d'un poste consulaire ou d'une mission diplomatique belge à l'étranger. Il a été créé à la fin des années 60 dans le département de la Fonction publique.

Après un fonctionnement empirique pendant près de quinze ans, son existence a été consacrée légalement en 1983. La loi de base sur le registre national est la loi du 8 août 1983 organisant un registre national des personnes physiques. Cette loi définit les missions du registre national, énumère de manière limitative les informations qui y sont enregistrées et la source de celles-ci, définit les conditions et la procédure pour obtenir l'autorisation d'accéder aux informations du registre national ou d'en avoir communication et d'utiliser le numéro d'identification. Cette loi fixe également les sanctions pénales que peuvent encourir les contrevenants à certaines dispositions. On peut donc réellement parler d'un dossier électronique de population.

La collecte des informations liées à l'identification d'une personne et l'attribution, dans le cadre de cette collecte, d'un identifiant unique intervient dès la naissance de la personne si les conditions fixées par la loi sont réunies. Elle peut aussi intervenir ultérieurement si la personne n'est pas née sur le sol belge et n'a pas été immatriculée auprès d'un poste diplomatique à sa naissance, mais vient s'y établir par la suite et répond aux conditions fixées par la loi pour être inscrite dans ledit registre.

Le dossier suit automatiquement la personne lorsqu'elle transfère sa résidence dans une autre commune ou, s'agissant d'un Belge, lorsqu'il va établir sa résidence à l'étranger et se fait inscrire dans les registres consulaires de population.

Le dossier électronique est lié à un identifiant unique, le fameux numéro d'identification au registre national qui a fait couler beaucoup d'encre. L'utilisation de cet identifiant n'est pas libre, elle doit être autorisée par le comité sectoriel du registre national depuis la modification de la loi sur le registre national intervenue le 25 mars 2003. Pour les autorités et organismes

disposant d'une telle autorisation, le numéro d'identification au registre national sert de clé dans le cadre des communications qu'elles nouent entre elles relativement aux personnes concernées et avec les personnes elles-mêmes.

L'introduction de la carte d'identité électronique en Belgique s'est faite dans une approche centrée sur le citoyen. En effet, en donnant à chaque citoyen un moyen légalement protégé d'identification qui lui permet non seulement de se faire reconnaître dans le cadre de ses relations dans le monde réel, de franchir les frontières au sein de l'Union européenne et de l'espace économique européen, mais aussi de nouer en toute sécurité des relations électroniques dans la sphère publique et dans la sphère privée, l'autorité publique a posé les premiers jalons vers un nouveau modèle sociétal intégrant les nouvelles technologies de la communication dans un cadre sécurisé, protégé, transparent et simplifié.

Voici un tableau représentant l'architecture de la gestion de l'identité en Belgique. Il comprend, d'une part, le service de l'État « à gestion séparée registre national – cartes d'identité » et le protocole de communication et le langage utilisé (interopérabilité *framework*), et d'autre part, les *identity policies*, qui sont les normes de base contenues dans la loi sur les registres de population, le *business process*, c'est-à-dire les applications registre national et cartes d'identité. Entre les deux, on trouve le *data model*, autrement dit les données proprement dites telles que décrites dans la loi du 19 juillet 1991 sur les registres de population et la loi du 8 août 1983 organisant un registre national des personnes physiques.

L'autorité de confiance chargée de l'identification de la personne physique est la commune. La source des données est le registre de population, source du registre national à la base de l'établissement de la carte d'identité.

Quant au processus de gestion des informations, le registre national est alimenté par les communes. L'information stockée au registre national est communiquée, redistribuée en fonction des autorisations légales vers les différents organismes et autorités ayant obtenu un accès.

Je ne m'attarderai pas sur l'architecture d'échange des données pour l'établissement des cartes d'identité.

L'utilisation de la carte d'identité représente-t-elle une menace pour la vie privée ? Certains le considèrent en évoquant que certains prestataires de service, agissant dans la sphère privée, peuvent à l'occasion, dans le cadre de

relations qu'ils nouent avec le citoyen client, inviter celui-ci à introduire sa carte d'identité dans un lecteur de cartes et ainsi prendre connaissance de toutes les données enregistrées sur la puce: nom, prénom, sexe, lieu, date de naissance, etc. ce qui leur permettrait de consulter, voire de conserver, à l'insu du citoyen, des informations à caractère personnel, sans respecter les principes de proportionnalité et de finalité.

Notre point de vue est que tout est une question d'équilibre. Le fait pour une personne d'accepter d'introduire volontairement sa carte d'identité, dans le lecteur de la carte, à la demande d'un tiers, avec lequel elle noue une relation, ne dispense pas naturellement ledit tiers de respecter les obligations fixées par la législation sur la protection de la vie privée. Je rappellerai simplement, sans m'y attarder, les notions de collecte loyale et licite pour des finalités déterminées, explicites et légitimes, etc.

Comparaison n'est pas raison. Pour avoir une estimation réelle de l'exactitude de l'équilibre entre le besoin d'un outil d'identité opérationnel et les garanties de la protection de la vie privée, il y a lieu de faire une comparaison entre les traces que nous laissons derrière nous dans le monde de l'internet. Certains sites nous donnent une indication très claire sur les informations dont les sites web disposent sur leurs utilisateurs telles que l'adresse IP, le type de fureteur (*browser*), le système d'exploitation de l'ordinateur et d'autres données qui les identifient de manière relativement précise.

Le sujet des caméras de surveillance a été abordé, je ne m'y attarderai pas. Je préciserai toutefois qu'une intrusion dans la vie privée, que l'on peut considérer comme plus importante, est à constater dans l'utilisation générale de caméras de surveillance dans les commerces et les lieux publics. C'est la réalité dans laquelle nous vivons.

Nous considérons que la transparence est le facteur clé de la protection et de l'équilibre dans le domaine de la protection de la vie privée. L'application pratique de la règle de proportionnalité à la carte d'identité doit être positionnée dans ce contexte. La carte d'identité est utilisée sur une base volontaire. Elle octroie un accès sécurisé à des services en ligne qui permet une certaine transparence pour le prestataire de services.

Certains estiment que les données transmises lors de la lecture de la carte d'identité devraient être limitées. L'avenir nous dira ce que nous devons en penser.

Une piste intéressante serait de considérer le citoyen comme partenaire dans la gestion de ses données d'identité.

Pour pouvoir utiliser pleinement les possibilités de protection de la vie privée offertes par l'identité électronique, nous devrions permettre davantage de transparence. Tel est déjà le cas pour les données du registre national. Vous savez en effet que tout citoyen peut consulter ses données au registre national au moyen de sa carte d'identité et prendre connaissance des consultations ou transactions effectuées sur son dossier au cours des six derniers mois. Selon nous, d'autres organismes publics devraient atteindre un même niveau de transparence.

Nous estimons donc que la carte d'identité électronique est un atout pour la protection de la vie privée. Dans le monde virtuel, elle protège l'individu contre l'usurpation de son identité, en lui donnant une identité de référence unique, attestée par l'État, sécurisée et protégée. En outre, elle rend possible l'indispensable transparence dans la gestion des données à caractère personnel, et permet de considérer le citoyen comme participant à la protection de ces données.

Les applications intégrant la carte d'identité sont de plus en plus nombreuses : eBay, etc.

Pour terminer mon intervention, je citerai le Livre blanc rédigé dans le cadre de la mission confiée en 2001 par le ministre français de la Fonction publique et de la Réforme de l'État à Pierre Truche, magistrat président honoraire de la Cour de cassation française et président de la Commission de déontologie et de sécurité, à Jean-Paul Faugère, préfet de Vendée, et à Patrice Flichy, professeur à l'Université de Marne-la-Vallée, en préparation au débat public sur les modalités de mise en œuvre des télé-services publics. Je vous sou mets ces quelques pistes de réflexion susceptibles d'alimenter un débat démocratique sur le sujet.

« Dans un univers où les fichiers administratifs ne sont plus simplement un danger pour la vie privée, mais avant tout un élément de la vie de chacun, permettant l'apparition de services privés et publics en ligne, de nouvelles attentes se préciseront. Puisque l'usage des réseaux se répand et que les services publics en ligne ne sont pas redoutés, mais attendus avec impatience, il ne suffira plus de protéger l'individu vis-à-vis des traitements de données, il faudra lui permettre de tirer parti de ces traitements de données.

Un nouveau droit qui garantirait, au-delà de l'accès et de la communication, la libre disposition des données, c'est-à-dire l'autodétermination par une personne de l'usage des données qui le concernent, pourrait ainsi s'esquisser. »

Cela constitue des pistes de réflexion.

En Belgique, l'application de « Mon dossier » a permis la mise en place d'un système de diffusion des données au citoyen. Grâce à l'application de « Mon dossier », le citoyen peut faire imprimer un extrait sous format Pdf, qui est signé par le registre national. Cet extrait a la même force probante qu'un extrait tiré des registres de la population. La loi du 27 avril 2007 a en effet modifié l'article 4 de la loi du registre national en vue de consacrer cette force probante de ses données.

J'en reviens au Livre blanc qui relève une nouvelle approche reposant sur la confiance réciproque : confiance de l'administration vis-à-vis des usagers, simplification administrative et confiance des usagers vis-à-vis de l'administration. Cette confiance dépend de la capacité des administrations à restituer aux usagers ce qu'elles détiennent sur eux. L'auteur précise : « Les formulaires imprimés ou numériques pré-remplis vont dans ce sens. L'utilisateur peut vérifier la pertinence de ce qu'une administration détient sur lui. L'administration pourrait ainsi, à partir de la connaissance de situations personnelles, informer les usagers sur les droits qu'ils peuvent exercer. »

La personne est-elle propriétaire de ces données ?

« La réponse est négative. Les données personnelles ne doivent pas être analysées en termes de droit de propriété car les personnes ne peuvent pas les modifier librement. La dévolution du nom, la détermination de l'état civil sont fixés par la loi. En outre, un droit de propriété peut être vendu, mais les droits de l'homme ne peuvent faire l'objet de transactions. Bien que la personne concernée ne soit pas auteur de l'information au sens de la mise en forme, elle est le titulaire légitime de ces données. Quand l'objet des données est un sujet de droit, l'information est un attribut de la personnalité.

La limite au principe de maîtrise des données peut être considérée comme suit : il ne saurait être fait obstacle à l'accomplissement d'objectifs d'intérêt public à caractère obligatoire. Cela serait également limité par les règles visant à protéger les personnes les plus vulnérables.

Cette maîtrise s'exercerait dans cette zone de latitude, ces cas et ces situations où la décision de communiquer ou non certaines données personnelles, d'autoriser leur transmission d'une administration à une autre peut avantageusement être laissée à l'initiative des personnes. »

Les auteurs du Livre blanc nous parlent également de l'évolution vers des comptes administratifs personnalisés et plusieurs scénarios sont possibles, comme le coffre-fort à distance, le coffre-fort à domicile ou la maison virtuelle de services publics qui seraient accessibles avec une clé unique, des clés multiples ou une combinaison de ces deux moyens.

La Belgique a déjà évolué car nous avons donné à la personne la possibilité de consulter les données que nous stockons au registre national grâce à une clé, à savoir sa carte d'identité électronique.

Pour conclure, je dirai que, depuis plusieurs années, la Belgique a compris l'importance de la question et a mis en œuvre un système rigoureux d'identification des personnes. Ce système a évolué au fil des années en intégrant les technologies nouvelles, tout en garantissant la protection de la vie privée.

L'introduction de la carte d'identité a permis de donner à tout Belge et, d'ici à deux ans, à la majorité des étrangers un outil leur permettant de s'authentifier et de signer en toute sécurité dans le cadre de leurs relations électroniques. Cet outil constitue une opportunité à saisir par celles et ceux qui, gérant des bases de données à caractère personnel, décideront de s'engager résolument dans la voie de la transparence pour une meilleure protection de la vie privée.

**M. Dechamps**, Rédacteur en chef de Citizen<sup>e</sup> – Nous accueillons M. Boland, Premier attaché juriste au Service juridique du Centre informatique pour la Région bruxelloise (CIRB) sur le thème des photographies aériennes et la protection de la vie privée.



## 8. Les photographies aériennes et la protection de la vie privée

■ **M. Boland, Premier attaché juriste au Service juridique du Centre d'Informatique pour la Région Bruxelloise (CIRB)**

– Je vais vous situer le contexte de mon exposé. Nous sommes partis de ce que nous avons vécu au CIRB qui, outre ses compétences informatiques générales, a des compétences en matière de cartographie. Qui dit cartographie dit aussi nécessité de mises à jour. Le meilleur moyen de réaliser une mise à jour cartographique en milieu urbain reste la photographie aérienne avec un certain nombre de techniques que j'aurai l'occasion de vous illustrer.

Ce faisant, on dispose d'un certain nombre de données fort intéressantes. Nous avons le projet de mettre ces données à la disposition du public, sur le site du CIRB, afin que chacun puisse consulter les photographies aériennes à une résolution de 60 cm et même voir avec une résolution de 10 cm son lieu d'habitation à condition de s'identifier avec sa carte d'identité électronique.

Les trois juristes qui travaillent dans ce centre d'informatique sont isolés parmi des informaticiens, des ingénieurs, des physiciens et des mathématiciens qui – pour caricaturer – fonctionnent avec un axiome selon lequel il faut avancer si les choses sont techniquement possibles. Pour caricaturer également les juristes, ces derniers fonctionnent sur un axiome un peu différent : ils font confiance si l'on estime que les choses sont possibles. Est-ce vraiment le cas ?

Dans le cadre de ce projet de publication des photos aériennes, s'agit-il d'un traitement de données à caractère personnel ? L'utilisation de données résultant de photos aériennes et leur diffusion tombent-elles sous le coup de la même loi ?

Dans la deuxième partie de mon exposé, je confronterai le résultat de cette réflexion avec une autre législation issue d'une directive européenne, la directive 2003/98/CE sur la réutilisation des données de l'administration.

Pourquoi les juristes du centre d'informatique pour la Région bruxelloise se sont-ils émus de la mise en ligne de données cartographiques puisque tout le monde peut y accéder sur le web grâce à *Google Earth* ?

L'accès à *Google Earth* ne va pas changer grand-chose à notre vie privée en proposant des vues de la Belgique. Au niveau de Bruxelles, les vues sont plus précises, mais la protection de la vie privée est néanmoins encore acceptable. Une vue plus oblique, plus précise, plus ciblée sur un bâtiment relève toujours du tolérable. *Google Earth* existe aussi en trois dimensions avec des vues obliques bénéficiant d'une résolution plus fine. Si on prend le cas de Hambourg, en croisant de façon informatisée les données de la photo avec d'autres données facilement disponibles, on arrive à un résultat plus significatif.

Aux États-Unis, grâce à *Google Map*, on peut avoir accès à des photos terrestres de villes américaines, ce qui est toujours acceptable et peut se comparer à un bon atlas.

La photo que je vous soumetts montre une rue de Denver, ce qui est aisément vérifiable en consultant, à partir d'un moteur de recherche, un annuaire des rues des villes américaines. Comme vous pouvez le constater, cette photo est très précise et peut nous donner beaucoup d'informations, concernant par exemple la saison en fonction de l'état de la végétation, l'heure en fonction de la longueur des ombres projetées par les bâtiments, etc. Nous disposons ainsi de données un peu plus gênantes, un peu plus troublantes, qu'il est possible d'affiner et, bien entendu, de comparer.

Pourquoi, contrairement à d'autres organismes, le CIRB a-t-il des états d'âme à cet égard ? Tout d'abord, comme toutes les autorités publiques, nous sommes soumis au principe de la légalité et nous devons dès lors nous demander si nous pouvions traiter ces informations. La question a fait débat. Nous nous sommes d'abord demandé si les données cartographiques étaient

des données à caractère personnel au sens de la loi de 1992. La réponse est bien entendu positive. C'est ce que la Commission de la protection de la vie privée a par ailleurs indiqué dans son avis n° 262 006 du 12 juillet 2006 ; elle a considéré que le traitement automatisé d'images satellites de propriétés de personnes physiques par le service de l'urbanisme devait être considéré, dans le cas qui lui était soumis, comme un traitement de données à caractère personnel. La loi sur la protection de la vie privée est dès lors d'application.

Nous sommes bien dans ce cas, puisque les données bénéficiant d'un certain degré de résolution permettent de localiser une personne identifiée ou identifiable. Il n'est pas nécessaire d'avoir une très haute résolution pour identifier quelqu'un ; un bon degré suffit.

Autre exemple de données disponibles sur Internet : grâce à *Microsoft Virtual Earth*, on peut par exemple voir l'hôtel bruxellois situé en face de la gare centrale. Comme vous pouvez le constater, le degré de résolution est, ici aussi, fort inquiétant. On peut facilement imaginer les informations qu'il est possible d'obtenir en croisant ces données avec d'autres bases de données, automatisées ou non, fort nombreuses sur l'internet.

Nous nous sommes donc interrogés à ce sujet en nous fondant sur le travail de base du CIRB. La finalité de notre traitement est de disposer d'un outil cartographique pour la Région. Cette finalité a une base légale. Comme je vous l'ai expliqué, nous procédons aux mises à jour à partir de photographies aériennes. Qu'aperçoit-on sur une photo aérienne ? Une succession de carrés et de rectangles plus ou moins rapprochés. C'est le plan de vol. Nous devons tenir compte d'un impératif technique : la courbure de la photo due à la lentille. La correction effectuée donne l'orthophoto. Une photo verticale est prise, pour les besoins de la mise à jour, à une époque de l'année où les arbres ont perdu leurs feuilles.

Nous nous étions demandés quelles informations utiles nous pourrions diffuser. De telles informations peuvent être utiles pour des projets d'urbanisme d'ensemble, de grands axes de pénétration, de répartition de chantiers, mais cela n'a pas beaucoup d'intérêt de les mettre à la disposition d'un large public sur un site internet. Par contre, ces photos aériennes, prises selon une certaine périodicité, vont permettre de comparer l'état des bâtiments dans une optique historique.

La résolution n'étant pas extraordinaire, elle ne permet pas d'identifier ce qui se passe sur le terrain ou dans l'arrière-cour de M. X ou Y. Le premier jeu

de photos que je vous montre date de 1996, il montre un très beau chantier. Trois ans plus tard, le quartier est déjà nettement plus urbanisé et en 2004, encore davantage. L'espace traité est très vaste et en glissant vers le bord supérieur gauche de la photo, on peut observer des propriétés beaucoup moins vastes et des propriétés privées.

Avant de faire la balance entre la finalité légitime, à savoir la mise à la disposition, sur la base de la Convention d'Arrhus, des données photographiques au public, et la protection de la vie privée, quel était l'intérêt pratique de les rendre publiques ? Si l'on reste à un niveau de résolution de deux mètres, cela ne présente aucun intérêt, pas même celui du flou artistique. En descendant à un mètre, on n'apprend pas grand-chose mais les contours se précisent. À soixante centimètres en revanche, l'image devient très nette.

C'était l'idée de départ du projet : mettre à disposition ce degré de résolution pour tout utilisateur de l'application. Cependant, cela devenait déjà problématique dans la mesure où l'on distingue parfaitement les contours, les ombres, ce qui permet de déterminer si l'on a construit ou détruit un bâtiment, si l'on a enlevé ou réaménagé une construction à l'intérieur d'un bâtiment. Autant de données qui deviennent extrêmement sensibles. Imaginez le degré de précision supplémentaire obtenu si l'on descend à vingt centimètres ! À dix centimètres, imaginez tous les croisements possibles avec d'autres bases de données et toutes les informations qu'on peut en tirer.

Sur cette base, nous avons une finalité légitime et une base légale, la Convention d'Arrhus. Nous devons faire la balance des intérêts avec la protection de la vie privée. Pouvons-nous accepter de mettre à la disposition des personnes physiques et des entreprises ces photos aériennes qui présentent un intérêt incontestable et ces applications qui fonctionnent bien ? Nous sommes arrivés à une conclusion négative parce que nous ne sommes pas parvenus à prouver que l'intérêt général l'emportait sur la protection de la vie privée. C'était tout le débat sur la proportionnalité lancé par le professeur Poullet.

Avec le matériel dont on dispose, il est possible d'utiliser une photo aérienne à un autre usage. Prenons par exemple une photo prise à Bruxelles, un matin à 8 h 45 m 55 s. On peut y identifier deux véhicules. Sur un cliché pris trois secondes plus tard, on peut à nouveau repérer ces deux voitures. Elles se sont déplacées. On peut constater qu'en trois secondes, le premier véhicule a parcouru 22 mètres; il s'est donc déplacé à 26 km/h. Le second n'a fait que 19 mètres et a donc roulé à 23 km/h.

Sur une autre photo, on peut constater qu'un citoyen s'est fait construire une piscine en forme de cœur. On peut voir qu'il y avait une personne au bord de la piscine à 9 h 34 m 5 s. On la retrouve à 9 h 45 m 52 s. Entre les deux, elle s'est déplacée de 5 mètres mais on n'a pas calculé sa vitesse.

Tout ceci constitue la partie ludique de mon exposé mais c'est basé sur des photos prises lors d'une campagne de photographies aériennes pour mettre à jour la carte Urbis. Vous voyez jusqu'où on peut aller avec ce genre d'outil.

Comment est-il possible de faire cohabiter certaines législations ? Comment peut-on effectuer la balance des intérêts ? Le système de photographies et les systèmes géographiques que je viens de vous montrer ne servent pas uniquement à faire de belles photos aériennes et à concocter des présentations intéressantes lors d'un colloque. Ils permettent aussi de se demander ce qu'on peut faire avec un système d'information utilisé par l'administration.

Il est par exemple possible de coller, sur une photo aérienne de rues, des données relatives à un linéaire de circulation. On peut ainsi enrichir un document brut avec d'autres informations. En sélectionnant et en agrandissant une partie de la photo, on obtient une vue plus précise. Il est dès lors possible de mettre des numéros sur les bâtiments et de compléter cette photo par un plan reprenant des données cadastrales. Voilà ce qu'on peut faire avec un système d'informations.

La directive UE2003/98 prévoit la mise à la disposition de tiers – essentiellement des entreprises – des données détenues par l'administration à des fins de réutilisation, c'est-à-dire pour la poursuite d'autres finalités que celles pour lesquelles ces données ont été recueillies. Ce texte prévoit très clairement qu'il ne porte pas préjudice à la directive UE1995/46 garantissant la protection de la vie privée. La Commission pour la protection de la vie privée a été interrogée par les législateurs qui ont tous, à l'exception du parlement de la Région de Bruxelles-Capitale, transposé cette directive. Ils souhaitaient savoir ce qu'il est possible de faire de ces données à caractère personnel.

La réponse a été sans équivoque par rapport au texte original qui prévoyait de ne pas révéler le contenu des données à caractère personnel qui s'y trouvaient. La commission a dit qu'il fallait rendre ces données anonymes, au sens de l'arrêté royal qui exécute la loi de 1992. Il ne doit pas être possible par un procédé inverse de connaître l'identité des personnes.

Nous avons donc, dans ce cas précis, un outil très complet et complexe développé pour les besoins de la cartographie. Mais son utilisation par le public nécessite des machines capables de supporter le logiciel et des compétences pour mettre en œuvre ces programmes, toutes choses dont le commun des mortels ne dispose pas. Mais la balance des intérêts et le débat auront lieu si on désire réutiliser cet outil.

Si l'on considère les possibilités cartographiques que je vous ai montrées, on pourrait conclure que le débat sera tranché en faveur de la protection de la vie privée. Quant à la réutilisation, au vu des systèmes d'information disponibles et de ce qu'ils peuvent produire comme données, elle me paraît fort difficile.

Je voudrais conclure en rappelant deux choses. Nous sommes face à deux directives, la 1995/46/CE et la 2003/98/CE, qui poursuivent des objectifs liés au traité européen. Il ne faut jamais le perdre de vue. Il s'agit de créer les conditions de développement d'un marché. Quand, en 1992, le législateur adopte la loi sur la protection de la vie privée, il agit en vue de protéger la vie privée des personnes physiques. La directive 1995/46/CE agit de la même manière, mais avec un autre but : créer les conditions de sécurité optimales pour la circulation de données à caractère personnel dans l'Union européenne en vue de la création du marché unique. Il en va de même pour la directive 2003/98/CE. Quand on fait la balance des intérêts entre la vie privée et la réutilisation, il ne faut jamais perdre de vue l'objectif poursuivi par les directives et leur champ d'application. Il ne faut pas diluer le problème dans un débat très général sur le plan des droits de l'homme et de la protection de la vie privée. Ma conclusion, c'est que, si l'on poursuit ces objectifs, la balance des intérêts doit se faire de manière encore plus stricte et rigoureuse.

**M. Verschuere.** – Je voudrais apporter une petite précision sur la finalité des directives européennes. L'Union européenne n'a pas pour but de jouer dans la cour des droits de l'homme, mais de privilégier et de faciliter le commerce. L'objectif de la directive 1995/46/CE est bien entendu de faciliter les échanges de données transfrontalières entre les pays de l'Union en créant une harmonisation de la protection des données personnelles dans chaque pays. Lorsqu'elle n'était pas la même partout, les flux transfrontaliers ne pouvaient pas se faire. Les deux sont donc liés. La directive n'est pas le dieu tout puissant auquel se référer en toute occasion. L'objectif consacré par cette directive, c'est de faciliter les flux en protégeant le droit des personnes.

**M. Boland.** – Je suis d'accord avec vous. Je me suis peut-être mal exprimé ou de manière incomplète. Ce que je voulais dire, c'est que les

directives ne sont pas toutes puissantes. C'est du droit dérivé des traités de l'Union. Je voulais simplement marquer les champs d'application et préciser que l'on peut tenir compte aussi d'une hiérarchie des normes par rapport à d'autres instruments internationaux, protecteurs justement des droits de l'homme et notamment de la vie privée. C'est cette nuance-là que je souhaitais introduire.

**M. Verschuere.** – En Belgique, c'est la loi belge qui s'applique, ou des instruments qui ont une applicabilité directe.

La bonne démarche est de s'interroger sur la manière de faire, sur ce que disent les informaticiens et sur ce que pensent les juristes. Ces derniers n'ont pas toujours raison. Les informaticiens savent faire beaucoup de choses. Les données à caractère personnel peuvent être rendues anonymes. Les cartes numériques sont nettoyables. Pouvez-vous rendre ces cartes diffusables ? Il y a peut-être un intérêt à le faire. Il ne faut pas réfléchir uniquement en terme de proportionnalité par rapport à des normes juridiques mais aussi par rapport à des capacités techniques que vous pouvez maîtriser.

**M. Dechamps, modérateur.** – Je suggère de poursuivre le débat après avoir entendu l'exposé de M. Jongen.

**M. Dechamps, modérateur, Rédacteur en chef de Citizen<sup>e</sup>** – La parole est à M. Jongen, médecin généraliste, pilote du groupe "droits d'accès" du Réseau Santé Wallon.



## 9. Réseau santé wallon et respect de la vie privée

### ■ *M. Jongen, Médecin généraliste, pilote du groupe "droits d'accès" du Réseau Santé Wallon*

– Je suis chargé de vous expliquer en quoi le Réseau santé wallon respecte ou non la vie privée. Si je suis ici plutôt qu'un informaticien ou un technicien du Réseau, c'est parce qu'on a jugé qu'un médecin généraliste était quelqu'un de particulièrement sensibilisé au droit du patient, au respect de sa vie privée et au respect du secret professionnel.

J'aborderai différents points. D'abord, l'origine et l'histoire du projet. Ensuite, sa couverture et sa représentativité. Je dirais aussi quelques mots sur son organisation et sur le cadre réglementaire et législatif. Je terminerai par une présentation pratique du Réseau santé.

Au départ, il existait un certain nombre d'associations télématiques médicales régionales. En Wallonie, il s'agit de l'Association carolorégienne de transmission hospitalière (ACTH) qui couvre la région du Hainaut et du Brabant wallon, de l'Association namuroise de télématique médicale (Anatem), de l'Association liégeoise de télématique médicale (Altem), de l'Association médicale de l'arrondissement de Verviers et de l'Est de la Belgique (Meditel).

Vous avez entendu parler du projet « S3 », Serveur de soins de santé, qui s'est arrêté fin 2005. Le pouvoir fédéral nous a proposé de reprendre le

projet. C'est ce que cet ensemble d'asbl de télématique a décidé de faire début 2006. Ce projet s'appelait *Flow Alpha* au niveau fédéral, *Flow Beta* en région de Bruxelles et *Flow Gamma* en région néerlandophone.

Quelle est la couverture du Réseau santé wallon et quelle est sa représentativité ? Actuellement nous avons cinq asbl télématiques, puisque nous en avons une supplémentaire pour la région de Tournai. La région d'Anatem s'est étendue à la province du Luxembourg. Nous avons aussi constitué une asbl faitière, la Fédération régionale des associations de télématique (Fratem) qui couvre 88 % des lits d'hôpitaux généraux de Wallonie. Cela représente 32 hôpitaux sur 44. J'ajoute que certains hôpitaux de Mons et de Bruxelles ne sont pas repris dans ce pourcentage.

La Fédération des associations de généralistes (FAG) a voté, le 15 décembre 2007, un soutien unanime au projet.

Dans chaque asbl télématique régionale, il y a 50 % de médecins spécialistes et 50 % de généralistes. Toute la médecine est ainsi représentée. Ce réseau en construction couvre pratiquement toute la Wallonie, à l'exception d'une petite zone autour de Braine-l'Alleud, une autre autour de Commines et une autre encore dans la région du Centre, qui va bientôt rejoindre le projet.

Le Réseau regroupe des médecins généralistes, des spécialistes, des kinés, des infirmières, les hôpitaux, etc. Ce sera une infrastructure de communication permettant l'échange de documents médicaux entre professionnels de la santé (dans un premier temps, uniquement entre médecins) pour assurer la continuité des soins aux patients.

Un document médical peut être un rapport de consultation, un protocole de laboratoire, un rapport d'hospitalisation, un dossier résumé d'urgence, etc.

Le Réseau santé wallon offre un cadre réglementaire explicite, un cadre organisationnel assurant la conception, le développement, l'opérationnalisation et le support d'outils techniques, la formation et le support aux patients et aux professionnels de santé, l'organisation d'une structure de surveillance indépendante et un ensemble d'outils informatiques permettant l'échange efficace et sécurisé de données pertinentes. Tout cela est très technique mais quand il s'agit du droit des patients, on ne peut s'écarter des définitions.

Le Réseau santé wallon n'est pas et ne sera jamais un dossier médical centralisé.

Le Réseau santé wallon vise avant tout à interconnecter les dossiers médicaux informatisés (DMI) des professionnels de santé, aussi bien dans l'hôpital qu'à l'extérieur. À l'exception du Sumehr (*Summarized Electronic Health Record* – dossier santé d'urgence), les documents restent exclusivement dans les DMI connectés. Le réseau ne communique aucun document médical, mais indique par un pointeur qu'il existe un document médical concernant tel ou tel patient sur le site de tel ou tel hôpital.

Pour assurer l'interconnexion des dossiers médicaux informatisés, le Réseau santé wallon propose les outils suivants :

- un serveur central sécurisé qui héberge les données ;
- une infrastructure de connexion sécurisée entre les DMI des hôpitaux et le serveur central,
- ainsi qu'avec les médecins extrahospitaliers généralistes et spécialistes ;
- des mécanismes d'inscription des patients et de gestion de leur consentement explicite ;
- des mécanismes d'inscription des professionnels de la santé et de gestion de leur consentement explicite ;
- des mécanismes de gestion des droits d'accès reposant sur l'existence d'un lien thérapeutique entre le patient et un professionnel de santé. Il y a un lien thérapeutique dès qu'il y a contact direct entre un patient et son médecin. Dès qu'une personne pousse la porte d'une consultation médicale, on peut considérer qu'il existe un lien thérapeutique et, avec l'accord du patient, ses données médicales seront encodées dans le Réseau santé wallon.

Sans lien thérapeutique, il ne peut y avoir gestion d'un dossier médical sur le réseau Santé wallon.

- Il existe également des mécanismes de traçage des accès et des consultations de l'historique de ces accès,
- et des signatures électroniques des transactions effectuées sur le réseau ;
- on dispose également d'un index sécurisé des patients ayant consenti au partage de certains de leurs documents
- et d'un index sécurisé des documents mis à disposition d'un service web permettant d'interroger, de consulter et de télécharger les documents.

- Enfin, des outils sont mis à disposition pour limiter la diffusion d'un document ou gérer la liste des destinataires.

Tous ces échanges sont standardisés au format KHMER, y compris le service web, afin de garantir la meilleure compatibilité avec les réseaux « santé » régionaux bruxellois et flamands, ainsi qu'avec les dossiers médicaux informatisés (DMI) de médecine générale.

Nous gérons uniquement la partie wallonne du pays mais, autour de Gand, un réseau santé en développement utilisera les mêmes standards. La Région bruxelloise prévoit de confier le développement d'un réseau santé à un partenaire privé qui utilisera les mêmes standards afin de garantir l'interopérabilité des systèmes.

La Fratem a élaboré la première version du règlement relatif à la protection de la vie privée. Le document, en gestation, comptera une quarantaine de pages. Il y a deux ans et demi, nous avons suivi une formation sur la télémédecine à la faculté de M. Pouillet. Nous avons en vain demandé de l'aide au fédéral pour ce qui concerne la protection de la vie privée. En l'absence de réponse satisfaisante, nous avons décidé de développer le projet par nous-mêmes. Cela représente un énorme travail. Pour fin avril, début mai, la version définitive pourra sans doute être soumise pour approbation à la commission de protection de la vie privée et à l'ordre des médecins.

Ce document décrit la façon dont le Réseau santé wallon se conforme aux prescriptions légales et déontologiques en matière de gestion de données de santé et de protection de la vie privée. Je fais ici référence à la loi du 8 décembre 2002 en matière de légitimité du traitement de données à caractère personnel. Le texte décrit explicitement les finalités, la responsabilité du traitement de données, la durée de conservation, le droit de la personne concernée, la confidentialité, la sécurité, la qualité des données et la publicité du traitement de données à caractère personnel. Le document indique aussi comment il respecte les obligations de l'arrêté royal du 13 février 2001 portant exécution de la loi relative à la protection en matière de codage et d'anonymisation des données dans le cadre d'analyse à des fins historiques, statistiques et scientifiques qui s'écarteraient de la finalité originale du traitement. En principe, le Réseau santé wallon s'interdit formellement de servir de base pour le traitement statistique de données médicales. Il n'en a d'ailleurs pas la capacité.

Structurellement, il est impossible de relever des données relatives à plusieurs patients. Le réseau n'est accessible que pour un seul patient à la fois.

Ce document explique encore comment le Réseau rencontre les obligations de la loi sur les droits du patient du 22 août 2002, notamment les modalités d'accès du patient à son dossier médical, aux annotations personnelles du médecin et aux données relatives à des tiers ; comment il respecte le secret professionnel, le code de déontologie médicale et plus précisément les recommandations de l'Ordre des médecins du 17 octobre 2005, l'avis du 26 juillet 2003 sur la loi sur les droits du patient et l'avis du 20 janvier relatif à la consultation directe de son dossier par le patient. Je rappelle que l'Ordre des médecins a considéré que le patient ne devait pas avoir accès seul à son dossier médical, mais qu'il pourra le faire en présence d'un professionnel de santé. Le Réseau respecte la loi du 8 août 1983, organisant un registre national des personnes physiques, la loi du 15 juillet 1990 régissant la Banque Carrefour de la sécurité sociale, la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique, le document de travail WP 131 du groupe de travail, article 29 de la directive européenne 1995/46 CE, ainsi que la loi du 20 octobre 2000 sur la criminalité informatique.

Certains principes fondamentaux régissent tous les accès aux documents médicaux du patient via le Réseau santé wallon.

- Il est interdit d'accéder aux documents d'un patient sauf si c'est nécessaire pour réaliser ou appuyer la réalisation d'une des finalités décrites au paragraphe 3 de notre document, à savoir ouvrir l'accès à des données et éventuellement constituer un dossier d'urgence.
- Dans ce contexte, le prestataire doit se limiter aux documents strictement nécessaires à la réalisation de sa propre mission
- et uniquement pendant la période requise à son exécution.
- Toutes les personnes qui accèdent à des documents médicaux du patient sont tenues par le secret professionnel.
- Aucune donnée ne peut être communiquée à des tiers, sous quelque forme que ce soit, en dehors de l'accord du patient.
- L'accès aux documents médicaux doit toujours être justifié par l'intérêt exclusif du patient. Ce principe est le maître-mot de l'organisation du Réseau santé wallon.
- Tous les accès aux documents sont « tracés » dans un fichier inaltérable, susceptible d'être consulté à la demande explicite du

patient par tout professionnel de santé disposant d'un lien thérapeutique avec celui-ci ou par le professionnel de la santé responsable de la surveillance du Réseau santé wallon.

- Le patient peut également accéder aux informations concernant le fichier de traçage.
- Tout abus peut donner lieu à de très graves sanctions judiciaires et disciplinaires

La gestion des droits d'accès a pour objectif de définir si un professionnel (P) de la santé est autorisé ou non à effectuer une action sur un objet (consultation d'un dossier, rapport d'hospitalisation, par exemple) en fonction d'un contexte donné.

Pour que la permission lui soit accordée, plusieurs conditions doivent être remplies.

- Le patient doit avoir explicitement consenti à l'échange de ces données via le Réseau santé wallon.
- Un professionnel de la santé doit avoir déclaré le document comme étant pertinent pour un échange. Dans notre exemple précédent, rien ne dit que toutes les données gynécologiques doivent se retrouver sur le Réseau santé wallon. Il en va de même des données psychiatriques.
- Cette déclaration ne peut pas avoir été assortie d'une exclusion spécifique d'un professionnel de la santé. Un document pourrait donc être publié sur le Réseau santé wallon et être visible par des médecins, mais pas par un professionnel exclu.
- Le professionnel de la santé doit avoir explicitement consenti aux règlements du Réseau santé wallon.
- Il doit avoir le droit d'effectuer l'action sur les objets (rapports d'hospitalisation, par exemple).
- Il doit avoir déclaré un lien thérapeutique légitime avec le patient (médecin traitant, par exemple).

Les principes de gestion des droit d'accès au Réseau santé wallon sont dérivés du modèle OrBAC, le plus avancé dans le monde médical.

Dans la pratique, la procédure commence par le consentement explicite du patient sans lequel aucun échange de documents médicaux n'est permis. Elle s'articule en deux étapes : l'inscription du patient et son consentement. L'inscription peut être réalisée soit directement par le patient au

moyen d'un formulaire sur Internet, soit par tout médecin au moyen du même formulaire ou par exportation depuis son dossier médical informatisé (DMlg). L'inscription peut également être effectuée dans un hôpital ou une polyclinique par exportation depuis le dossier médical hospitalier (DMlh), et par l'administration du Réseau santé wallon sur demande écrite du patient.

Pour que l'inscription soit effective, le patient doit exprimer son adhésion explicite au règlement du Réseau santé wallon. Ce consentement est matérialisé soit par une signature électronique via Internet, soit par une signature manuscrite d'un formulaire papier qui doit être renvoyé au Réseau santé wallon pour y être scanné et conservé.

C'est alors seulement que le patient sera connu pour l'échange de données sur le Réseau.

Le patient peut révoquer ces autorisations. Il peut superviser les droits d'accès : exclure un médecin, en autoriser un autre, révoquer une autorisation à tout moment. L'inscription et le consentement du professionnel de la santé seront gérés de manière analogue.

Je vous renvoie au site du Réseau santé wallon, où vous trouverez le règlement *in extenso*. La version définitive sera publiée après approbation par la Commission de la protection de la vie privée et par l'ordre des médecins. <http://www.reseausantewallon.be/reglementvieprivee.pdf>

\*\*\*

**M. Dechamps, modérateur.** – Je vous propose de passer à la séance des questions et réponses. Nous commencerons par les questions qui s'adressent à Mme Rouma.

**Pierre Crosse.** – Je travaille pour une société de services en logiciels libres. J'ai travaillé entre autres pour le projet : [monservicepublic.fr](http://monservicepublic.fr) que vous avez cité tout à l'heure. Il y a une différence majeure entre ce projet et la carte d'identité que vous nous avez présentée. D'un côté, on a une identification centralisée basée sur un identifiant unique et de l'autre, une identité fédérée basée sur un standard établi. C'est très différent du point de vue du cloisonnement des données. Quand j'utilise une identité fédérée je suis sûr qu'aucun fournisseur de service ne pourra utiliser des données qui ne lui sont pas destinées. Il n'a aucun moyen d'échanger des informations avec un autre

fournisseur de services. Quand j'ai une identité centralisée et un identifiant unique je me pose beaucoup plus de questions.

Comment s'assure-t-on que les données sont réellement cloisonnées avec la carte d'identité électronique ?

Concernant les entreprises privées, quelle confiance puis-je accorder à des entreprises comme Microsoft, par exemple, qui ont un pouvoir exorbitant puisqu'elles détiennent mon identité que je le veuille ou non. Comment suis-je sûr qu'on va pouvoir changer ses prestataires sans trop de coûts à moyen terme s'ils ne donnent plus satisfaction ? La réponse c'est : le recours aux standards, ce qui veut dire que j'ai la maîtrise complète du code si je ne suis pas content.

Je ne suis pas très rassuré quand je sais que ces entreprises, condamnées par la justice en Europe ou aux États-Unis, sont les dépositaires de mon identité. J'ai bien entendu tout à l'heure que l'on disait que le fait de mettre ma carte dans un lecteur ne dispensait pas de respecter la loi ! Dans le cas inverse, je dois respecter la loi aussi ! C'est une garantie un peu légère.

Je terminerai par une remarque. Vous avez fait un raccourci assez saisissant en juxtaposant *tax-on-web* et *eBay*. La carte va juxtaposer des services qui relèvent des compétences de l'État, émanation de la souveraineté populaire, et des services qui sont le fruit de prestataires commerciaux. Quand on ravale l'État au rang de prestataire de services, on transforme le citoyen en client ! Cela ne me paraît pas souhaitable dans des sociétés où on se plaint d'un déficit démocratique et d'un manque de conscience politique!

**Mme Rouma.** – La carte d'identité électronique est un moyen d'accéder à ses propres données. Il ne faut pas confondre la carte d'identité et les données stockées au registre national qui le sont dans un cadre légal, bien défini. Les données d'identification enregistrées sur la carte d'identité électronique proviennent de cette source authentique qu'est le registre national mais il ne faut pas les confondre.

**M. Verschuere.** – Je voudrais apporter quelques précisions à la question qui a été posée. Il y a trois concepts : l'identité, l'identification et l'authentification de l'identité. La carte d'identité électronique comporte des données personnelles qui n'ont pas de caractère secret. Cependant, la carte d'identité électronique n'est pas un identifiant, c'est un authentifiant de l'identité. Quelle garantie puis-je avoir, si je me connecte sur *eBay* ou sur des

sites de Microsoft, qu'on ne capte pas mes capacités d'authentification de mon identité après avoir « craqué » le code secret de ma carte d'identité ? Le problème réside dans la sécurisation de l'authentification.

**M. Mansvelt.** – La carte d'identité est un système asymétrique. L'identité qui se trouve sur la carte peut être accessible à tous. Il ne s'agit que du nom, des prénoms, de l'adresse et de quelques autres renseignements anodins.

Si vous surfez sur un site comme eBay, votre identification correspond à une signature électronique qui nécessite trois éléments : la carte d'identité dans le lecteur, le *middleware* de l'organisme certificateur et le code secret. Ce système est unique et la clé change à chaque utilisation. Le code Pic public change chaque année et ne peut être copié.

Par contre, si les informations émanant des services du ministère de l'Intérieur sont contrôlables, je crains que des organismes privés puissent ajouter d'autres informations auxquelles l'utilisateur n'aurait pas accès. C'est ainsi que toute personne ayant un compte bancaire doit fournir son identité à sa banque. Comment puis-je être certain que la banque n'introduit pas le solde de mes dernières opérations bancaires sur ma carte d'identité sous une forme non lisible ?

**M. Dechamps, modérateur.** – Est-ce techniquement possible ?

**M. Mansvelt.** – Oui, car aujourd'hui, sur la carte d'identité, une petite zone seulement est utilisée par l'administration. Il est donc possible d'inscrire d'autres informations. À cet égard, certaines banques, pour ne pas devoir travailler en ligne et vérifier l'opération bancaire effectuée, ce qui est onéreux, ont émis le souhait de pouvoir travailler hors connexion, en diminuant ainsi le coût de leur investissement par deux ou trois. Il faut aussi savoir que, dans quelque temps, la carte d'identité sera confondue avec la carte SIS.

Qu'en sera-t-il quand nous irons chez le pharmacien pour acheter tel ou tel type de médicament spécifique ? Si vous prenez un médicament utilisé pour la chimiothérapie, par exemple, on pourra en déduire que vous souffrez d'un cancer. Un garde-fou est prévu concernant la carte SIS : vous n'entrez dans la Banque Carrefour des soins de santé que par votre numéro de registre national. L'information ne figure pas sur la carte d'identité, mais se trouve dans une base de données. Votre signature n'est qu'une clé d'accès. La philosophie est donc différente et garantit précisément l'indépendance.

**M. Dechamps, modérateur.** – La parole est à Mme Rouma.

**Mme Rouma.** – Je ne suis pas techniquement en mesure de vous donner la réponse appropriée, mais mon collègue ici présent pourra vous apporter quelques explications.

**M. Roelandt.** – Je travaille au Registre national. Vous évoquiez l'ajout d'informations sur la carte d'identité. Dans quelques mois ou quelques années, je l'ignore, la carte d'identité sera dotée d'une puce qui rendra peut-être la chose réalisable. Pour le moment, un tel ajout est impossible.

Vous dites que le numéro national sert d'accès à la Banque Carrefour de la sécurité sociale. C'est aussi le cas pour le registre national. La carte d'identité est un moyen de vous identifier par rapport à une application. Lorsqu'il s'agit d'accéder à des données qui doivent être protégées en raison de leur caractère personnel, il faut utiliser d'autres moyens, plus sûrs.

**M. Dechamps, modérateur.** – La parole est à M. Pouillet.

**M. Pouillet.** – Je voudrais revenir sur les possibilités offertes par l'authentification numérique par rapport à l'authentification « vivante » de la personne.

Lorsque je suis dans le monde classique, traditionnel, je m'authentifie par ma personne. En d'autres termes, je signe. C'est un geste de la main. L'authentification numérique permet une dissociation : c'est à travers un prestataire de service de certification qu'il est possible de relier l'identité d'une personne à une signature.

Comment se fait-il que la Belgique n'ait pas exploité l'idée que, vivant dans un monde électronique, nous devons diversifier les méthodes d'authentification électronique ?

Le citoyen sera bien entendu mieux protégé s'il peut s'identifier de diverses manières. Ce principe est appliqué par Microsoft et par les gouvernements autrichien et danois, par exemple.

Au contraire, la Belgique a opté non seulement pour un numéro de registre national unique, mais aussi pour une signature électronique qui vaut autant pour l'administration que pour les entreprises privées.

C'est un risque qu'on n'aurait pas dû prendre. Comme l'a fait remarquer M. Verschuere, comment ces décisions ont-elles pu être prises ? Dans le silence des cabinets ? Par un certain nombre d'experts ? En tout cas, nous le savons, sans débat public.

**Mme Rouma.** – Le registre national n'a rien imposé. La carte d'identité électronique est explicitement reconnue par la loi du 25 mars 2003, qui a fait l'objet d'un débat démocratique. C'est le parlement qui a voté la loi. La diversification des moyens d'authentification devrait être approuvée par les représentants de la nation, dans le cadre d'un débat démocratique.

L'introduction de la carte d'identité électronique a été réalisée dans le cadre de l'*e-gouvernement*. On a ainsi donné à chaque citoyen la possibilité de s'authentifier et de signer électroniquement de manière sécurisée. On peut effectivement rouvrir le débat et diversifier les moyens d'authentification, mais cela doit être fait dans un cadre démocratique, à l'instigation des autorités politiques. Ce n'est donc pas l'administration qui est à l'origine de la mise en circulation de la carte d'identité électronique.

En citant le Livre blanc, je n'ai pas voulu dire que ce qui est fait en France est identique à ce qui se pratique en Belgique. Nous avons régulièrement rencontré des délégations du Sénat français. Nous recevrons d'ailleurs dans quinze jours une délégation française dans le cadre du débat sur l'introduction de la carte d'identité électronique. Nos approches sont différentes, mais j'ai trouvé intéressant de vous faire part des pistes qui ont été proposées dans l'étude réalisée pour le parlement français.

**Un participant.** – Je travaille pour la médiatrice de la Communauté française. Dans le cadre de la protection de la vie privée, on oublie souvent le problème de l'accès aux documents administratifs par les citoyens. Il en va de même pour les liens entre les avis de la Commission de la protection de la vie privée et ceux des différentes commissions d'accès aux documents administratifs. Quels sont les critères servant à définir les bases de données ? Peut-on y avoir accès et à quelles conditions ? Je pense notamment à l'administration fiscale.

On parle beaucoup de la protection de la vie privée. Il faut voir comment cela se passe concrètement. Des recoupements se produisent, avec ou sans contrôle. Des sélections de personnes ont lieu sur la base de déclarations d'impôt et de croisements de bases de données.

Je m'interroge donc sur ce qui peut assurer un certain équilibre. Des textes internationaux existent et il y a profusion de jurisprudence en la matière. Je crois que nous nous sommes un peu trop concentrés sur la protection de la vie privée. Travaillant dans un service de médiation, je peux vous dire que ce qui intéresse les gens, c'est d'accéder aux documents et de connaître leur contenu.

La Communauté française a voté dernièrement un décret sur la réutilisation d'une série de données. Mais, à ce jour, il n'y a eu aucun arrêté d'application du gouvernement.

**M. Dechamps, modérateur.** – La parole est à M. Verschuere.

**M. Verschuere.** – C'est un long débat. Les gens ont accès à leurs documents administratifs, ce sont des données qui leur sont personnelles. Oublions cette notion de vie privée, on ignore ce qu'elle recouvre. Parlons plutôt de données personnelles.

Je reviens brièvement aux données géographiques. La démarche des auteurs du projet est prudente et rigoureuse. Ils doivent continuer à y réfléchir. La loi n'est pas une frontière mais bien un guide qui force à la réflexion, y compris sur la définition d'une donnée personnelle protégée. Un numéro sur un bâtiment de rue est-il protégé ? S'il est mis en rapport avec une personne, il est protégé. Il faut réfléchir à chaque enjeu auquel on est confronté. Cela permet de déployer les politiques publiques de manière rigoureuse. Il ne faut pas non plus être bloqué par des réflexions strictes. C'est une loi d'encadrement et non d'interdiction.

**M. Dechamps, modérateur.** – La parole est à Mme Devos de l'Agence pour la simplification administrative.

**Mme Devos.** – Je voudrais revenir à l'intervention qui a précédé celle de M. Verschuere.

Comme Mme Rouma l'a indiqué, on peut avoir accès à un dossier du registre national. Il y a notamment le programme *My minfin* pour les informations fiscales, et le *Private search* pour les informations sur les entreprises.

Je voudrais connaître les possibilités d'avoir un rapport sur le nombre de citoyens qui demandent des informations au registre national. Ne pourrait-on regrouper les différentes possibilités de *My minfin*, *Private search*, etc., et avoir une réglementation ou des rapports d'évaluation communs pour répondre aux besoins des gens?

Je voudrais également poser une question à M. Boland qui a tenu un discours différent des autres. Il a notamment dit qu'un service public ne pouvait pas enfreindre la loi. Cependant, les entreprises privées sont aussi soumises à la loi et elles ne sont contrôlées que sur la base de plaintes. Or, je suis bien placée pour savoir qu'un très grand nombre d'entreprises réutilisent des données en totale illégalité, parfois avec des licences et des marchés publics. On les laisse faire, un peu par habitude. On n'agit contre elles qu'en cas de plainte.

**Un intervenant,** – Il y a une directive européenne.

**Mme Devos.** – Oui, mais une entreprise privée qui utilise des données publiques auxquelles elle a accès fait ce qu'elle veut.

**Un intervenant,** – Vous êtes fonctionnaire, dénoncez-la au parquet!

**Mme Devos.** – Je ne peux pas car je ne suis pas propriétaire des données. J'ai saisi la Commission de la protection de la vie privée en son temps. Des entreprises se trouvent dans ce cas-là et les citoyens concernés ne se plaignent pas. Google et Covast, sont en infraction, mais cela arrange parfois les gens sur qui portent les données.

Il ne faut pas diaboliser la directive 2003/98 car elle prévoit, dans un libre marché, de développer le marché intérieur dans un régime très libéral de libre concurrence, de transparence et de non-discrimination. Elle n'oblige pas les services publics à mettre ses données à disposition. Je conseille que le comité de la transparence que nous avons créé à l'échelon fédéral, auquel vous serez convié si vous le souhaitez, définisse les données publiques que chaque service public accepte de mettre à la disposition d'entreprises ou de tiers en vue d'une commercialisation. Vous n'êtes jamais tenu de le faire et je vous conseille de vous abstenir en cas de doute. Cela ne règle évidemment pas tous les problèmes car il y aura des pressions.

— *Les travaux du colloque se terminent à 15 h 50.*



## Table des matières

<b>Introduction</b>	p. 3
par M. Dechamps, <i>modérateur, Rédacteur en chef de Citizen<sup>e</sup></i>	
<b>1. La vie privée, un enjeu fondamental pour la démocratie</b>	p. 5
par M. Poullet, <i>Professeur aux Facultés Universitaires Notre-Dame de la Paix (FUNDP), Directeur du Centre de Recherches Informatique et Droit (CRID) et du FUNDP</i>	
<b>2. Pédagogie, assistance et contrôle : les missions de la Commission de la protection de la vie privée au bénéfice des services publics</b>	p. 17
par M. Verschuere, <i>Président de la Commission de la protection de la vie privée</i>	
<b>3. Présentation générale du modèle de la « Banque Carrefour »</b>	p. 23
par M. Quintin, <i>Administrateur général adjoint de la Banque Carrefour de la Sécurité sociale</i>	
<b>4. Politique nationale de sécurité de l'information : définition des enjeux</b>	p. 31
par M. Huet, <i>Conseiller en Chef de la Sécurité de l'Information du Service public fédéral Technologie de l'Information et de la Communication (FEDICT)</i>	
<b>5. La politique de sécurité de la Région wallonne</b>	p. 43
par M. Cornet, <i>Commissaire-adjoint en charge de la simplification administrative et e-gouvernement en Région wallonne (EASI-WAL)</i>	
<b>6. Analyse des risques à la Communauté française</b>	p. 51
par M. Martin, <i>Conseiller en Procédure et Sécurité, Entreprise publique des Technologies Nouvelles de l'Information et de la Communication de la Communauté française (ETNIC)</i>	
<b>7. L'organisation de la gestion de l'identité en Belgique</b>	p. 65
par Mme Rouma, <i>Responsable du Registre national</i>	
<b>8. Les photographies aériennes et la protection de la vie privée</b>	p. 75
par M. Boland, <i>Premier attaché juriste au Service juridique du Centre d'Informatique pour la Région Bruxelloise (CIRB)</i>	
<b>9. Réseau santé wallon et respect de la vie privée</b>	p. 83
par M. Jongen, <i>Médecin généraliste, pilote du groupe "droits d'accès" du Réseau Santé Wallon</i>	



Dépôt légal : D/2008/10.353/1  
Editeur responsable : Christian DAUBIE,  
Parlement de la Communauté française de Belgique  
Wallonie-Bruxelles  
1012 BRUXELLES.

