Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La vie privée, un enjeu fondamental pour la démocratie

Poullet, Yves

Published in:
Traitement et protection des données des administrations publiques, principes et moyens

Publication date:
2008

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 2008, La vie privée, un enjeu fondamental pour la démocratie. Dans *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.* Parlement de la Communauté française , Bruxelles, p. 5-16.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 20. Apr. 2024

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

1) l'usager 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'usager participe de lui-même à ces opérations, les déclenche et en contrôle l'usage.

2) l'usager 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'usager et des documents administratifs. Rien n'empêche alors que cet espace permette le traitement des "dossiers" communs à l'usager 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 31*bis* 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 télématique médicale, 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 diplômes, 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[e] – 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[e] – 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 mutuellisation informatique, de la théorie à la pratique. Aujourd'hui, nous parlerons du traitement et de la protection des données des administrations.