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

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Administration électronique

Poullet, Yves

Published in:
Droit de l'administration électronique

Publication date:
2011

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 2011, Administration électronique: le cas belge. Dans *Droit de l'administration électronique.* Académia Bruylant, Bruxelles, p. 327-343.

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: 16. Apr. 2024

ADMINISTRATION ÉLECTRONIQUE : LE CAS BELGE

PAR

YVES POULLET

PROFESSEUR AUX FACULTÉS DE DROIT DE NAMUR ET DE LIÈGE
DIRECTEUR DU CRID DES FUNDP
HTTP://WWW.CRID.BE

1. Nul ne songe à contester, en Belgique comme ailleurs, les bénéfices de l'administration électronique. Elle contribue en interne à une meilleure efficacité du travail administratif tant en rapidité qu'en qualité. Dans la relation administrations-citoyens, elle constitue un outil tant de simplification que de transparence administrative. La vision traditionnelle de l'information administrative en «silos», où chaque administration dispose de ses propres informations et de ses propres outils de traitement et où les communications entre administrations sont rares et sévèrement réglementées, cette vision a vécu au profit d'administrations en réseaux (au pluriel). On rappellera cependant que la vision classique du cloisonnement administratif a toujours été présentée comme la garantie offerte au citoyen d'une protection de ses libertés contre un Etat omniscient et omnipotent (1).

L'utilisation des technologies de gestion et de communication d'une information de plus en plus normalisée et autorisant donc des traitements interopérables (via les protocoles internet, l'utilisation du langage XML et de l'Universal Message Engine), crée, c'est indéniable, une potentialité d'intégration fonctionnelle des différentes entités administratives.

(1) A ce sujet, lire le rapport LASSERRE, *L'Etat et les technologies de l'information et de la communication. Vers une administration à accès pluriel*, Paris, La documentation française, 2000 : «L'accroissement des possibilités de la circulation de l'information modifie l'échelle des risques pour la protection des données dans la mesure où cet accroissement ressuscite la crainte d'un 'Big Brother'».

2. Nos gouvernements belges (2), en particulier au niveau fédéral, ont rapidement été séduits par les perspectives qu'offre l'administration électronique. Les applications nées des technologies de l'information et de la communication permettent de rationaliser le fonctionnement et les coûts des administrations et de se doter des outils nécessaires d'aide à la gestion et au contrôle de la politique publique, applications dites de back office. Le volontarisme gouvernemental est sans doute moins évident lorsqu'il s'agit de disposer d'outils de simplification et de transparence administrative dans la relation administration – administrés (le front office). Les services électroniques administratifs aux citoyens ont en effet quelque peine à démarrer.

3. L'e-gouvernement belge, cité volontiers en exemple par les autorités européennes, s'appuie sur deux précédents l'un des années 80, le registre national; l'autre des années 90, la Banque-carrefour de la sécurité sociale (BCSS) qui trouvent aujourd'hui leur pleine signification mais également révèlent leurs pleins enjeux et risques. Notre propos s'appuiera sur le rappel de ces deux précédents : le premier est à la base de la notion de source authentique, des numéros uniques d'identification et par là de procédé d'authentification et de signature; le second nous permettra d'approcher les multiples réseaux sectoriels et la manière dont la protection des données s'organise autour de ces réseaux. Enfin, sous ce second point, nous dirons un mot sur la façon dont la Belgique fédérale développe, nonobstant un fédéralisme de plus en plus poussé, une conception intégrée des réseaux des administrations relevant de ses diverses composantes.

(2) Pour une analyse complète mais peu récente, H. VAN SEBROECK, *E-GOV : Vers une administration électronique en Belgique*, Bureau fédéral du Plan, Working Paper, 4-01, Juillet 2001, disponible sur le site du Bureau du Plan : http://www.plan.be. Cf. également , I. DEPREST - F. ROBBEN, *E-Government : The Approach of the Belgian Federal Administration*, FEDICT-CBSS, Juin 2003, disponible à partir du site de l'ICRI : http://www.law.kuleuven.ac.be/icri/frobben/publications/2003%20-%20Egovernment%20paper%20v%201.0.pdf. Le lecteur consultera également le site de FEDICT (administration fédérale en charge du développement et de la coordination des applications de l'e-gouvernement au niveau fédéral, citée *infra*, n° 18) : http://www.fedict.be.

I. – DU REGISTRE NATIONAL À LA SOURCE AUTHENTIQUE

1. – *Le (ou les) numéro(s) d'identification : éléments d'un débat*

4. Dès 1983, la loi sur le registre national (3) attribuait à chaque citoyen belge un numéro dit de registre national et envisageait ce registre comme, ce qu'il est convenu d'appeler aujourd'hui, une «source authentique». Nous reviendrons sur cette dernière notion (*infra*, n°s 7 et s.). Le numéro de registre national est rapidement devenu le numéro unique de l'administration, tous secteurs confondus, tant celui de la sécurité sociale, que celui des finances. Aujourd'hui, ce numéro s'avère être l'outil qui facilite l'interconnexion de tous les fichiers au sein de l'administration d'autant plus qu'au sein des administrations, ce numéro constitue la clé d'accès des fichiers. La donnée «numéro d'identification du registre national» est incontestablement une donnée à caractère personnel. Son caractère d'identifiant unique, en particulier en Belgique où, contrairement à la plupart des autres pays européens (4), il n'existe pas d'identifiants sectoriels, justifie la mise en œuvre des mesures particulières proposées par l'article 20 de la directive européenne 95/46/CE. Cet article impose des contrôles préalables à la mise en œuvre de traitements susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées (5). Dès 1996, à propos de la carte de sécurité sociale et de l'inscription en clair du numéro de registre

(3) Loi du 8 août 1983 organisant un registre national, *M.B.*, 21 avril 1984. Cette loi a été à de nombreuses reprises modifiée. Nous reviendrons sur les modifications récentes de la loi du 25 mars 2003 (*M.B.*, 28 mars 2003).

(4) Cf. sur ce point, le très intéressant «*Document de travail sur l'administration électronique*», Groupe de travail de l'art. 29, 8 mai 2003, WP 73 disponible sur le site de la Commission européenne.

(5) Cette disposition européenne est traduite maladroitement par l'article 17*bis* de notre loi qui prévoit que «*Le Roi détermine, après avis de la Commission de la protection de la vie privée, les catégories de traitement qui présentent des risques particuliers au regard des droits et libertés des personnes concernées, et fixe [...] des conditions particulières pour garantir les droits et libertés des personnes concernées*». La disposition insérée entre la disposition relative à l'obligation de déclaration et celle relative au registre public pourrait sous-entendre que le Roi doit limiter son intervention à requérir des compléments de déclaration (et à la nomination d'un préposé conformément à l'alinéa 2 de cet article), ce qui est largement insuffisant et ne correspond pas à la volonté du législateur européen qui réclame des garanties de tout type et surtout un débat si possible public par rapport à ces traitements dits à hauts risques.

national au verso de cette carte (6), un débat parlementaire était réclamé par la Commission de protection de la vie privée (7). Ce débat n'a jamais eu lieu et la loi du 25 mars 2003 qui réforme la loi du 8 août 1983 organisant un registre national des personnes physiques fait figurer le numéro de registre national sur la carte d'identité tant de manière visible que lisible par lecture électronique, sans s'interroger sur les risques de diffusion de ce numéro bien au-delà des seules personnes autorisées à l'utiliser.

5. Le numéro unique facilite également la collecte et le dialogue de l'administration tant avec le citoyen, lui-même source d'informations à son propos qu'avec d'autres sources d'informations, comme l'entreprise, lorsqu'elle engage un nouvel employé et le déclare en se référant au numéro de registre national de ce dernier ou comme le pharmacien qui transfère la demande de remboursement de soins des patients en indiquant leur numéro de registre national.

Le caractère unique et omni-sectoriel de cet identifiant ne cesse d'inquiéter les défenseurs des droits de l'Homme. La généralisation de son utilisation au sein de l'administration et dans ses relations avec l'extérieur est contagieuse vis-à-vis du secteur privé. Les entreprises voire tous les organismes privés sont tentés d'utiliser également ce numéro dans leurs relations avec leurs clients (ainsi une école vis-à-vis de ses étudiants) et dans leurs relations entre elles. En toute hypothèse, n'ont-elles pas une base légitime à détenir ce numéro ? Ainsi, les banques ont l'obligation de vérifier l'identité des

(6) Avis n° 19/2002 sur la réforme du registre national, 10 juin 2002 (rapporteur Y. POULLET) disponible sur le site de la Commission de la protection de la vie privée : «*Plus fondamentalement, la Commission constate que, si l'adresse n'est plus visible à l'oeil nu sur la carte (seulement en lecture électronique), la carte reprend désormais de manière visible des données nouvelles, en particulier le numéro d'identification du registre national, au motif que celui ci est déjà repris sur la carte SIS et surtout que son utilisation est désormais libre. La mention du numéro de registre national «à l'extérieur» de la carte est inévitable, puisque ce numéro doit être utilisé, sous certaines conditions, par le titulaire de la carte en relation avec certaines institutions autorisées à utiliser le numéro de registre national. Afin d'éviter que le numéro de registre national soit communiqué à des instances qui n'ont pas le droit de l'utiliser, il est nécessaire de réserver l'utilisation de la carte d'identité électronique aux instances qui disposent bien de ce droit. D'une manière générale, la Commission invite le législateur à se pencher avec attention sur l'impact de la modification des mentions visibles sur la carte d'identité électronique. Elle rappelle qu'à propos de la mention du numéro d'identification sur la carte SIS elle avait souhaité dans l'avis d'initiative pris à l'époque (avis n° 12/97 du 30 avril 1997) un large débat sur cette mention. Elle constate que ce débat n'a pas eu lieu et souhaite attirer l'attention du Parlement sur les enjeux d'une telle libéralisation de l'utilisation du numéro*».

(7) Ce débat a eu lieu dans les pays qui nous entourent. Ainsi, aux Pays-Bas, où le projet d'identifiant unique a été abandonné au profit des identifiants sectoriels et en France où le Forum des droits sur l'Internet a été chargé d'animer un débat national sur la carte d'identité électronique (voir à cet égard, le site du Forum : http://www.foruminternet.org).

personnes demanderesses d'un compte en banque, ne peut-on dès lors justifier qu'elles conservent cette donnée et l'utilisent vis-à-vis des autres banques ou partenaires.

Bref, ces organismes privés ne doivent-ils pas déjà de toute façon, utiliser ce numéro dans leurs relations avec l'administration et le numéro de registre national ne s'arbore-t-il pas tant sur la carte d'identité que celle de sécurité sociale ?

6. Une réaction s'amorce cependant progressivement (8). On annonce la création d'un numéro santé (9) et d'un numéro fiscal (10) distincts du numéro de registre national qui par ailleurs n'apparaîtrait plus sur nos cartes d'identité.

Ajoutons que l'idée d'identifiant unique s'est élargie, au-delà du monde des personnes physiques, à celui des «entreprises», notion conçue de manière large, avec la loi du 16 mars 2003 créant la Banque carrefour des entreprises (en abrégé, la BCE) (11) et le gou-

(8) A noter sur cette question des identifiants uniques, la réflexion de la CPVP dans son avis sur la réforme du registre national (Avis n° 19/2002 , 10 juin 2002, rapporteur Y. POULLET) : «*Au-delà de cette première remarque, la Commission s'interroge sur la nécessité de prévoir des numéros sectoriels pour des données sensibles. Lors de son récent avis à propos de l'arrêté royal fixant les normes auxquelles doivent répondre le programme de soins pour les soins oncologiques et le programme de santé en matière d'oncologie (avis n° 14/2002) du 8 avril 2002, la Commission a prôné pour les données de santé l'utilisation d'un numéro de santé distinct de celui de sécurité sociale et ce afin de garantir une certaine étanchéité des circuits d'informations entre les deux types de données. Cet avis s'inscrit dans la volonté gouvernementale (Cf. déclaration des Ministres Vandenbroecke et Alvoet) de prévoir un 'Patient Identification Number' distinct du numéro de sécurité sociale. On pourrait de même dans le secteur des données judiciaires et de police prévoir l'obligation d'utilisation de numéros distincts. En d'autres termes, le projet devrait prévoir que pour des secteurs particuliers utilisant des données sensibles, l'utilisation de numéros spécifiques et des règles d'accès particulières soient imposées*».

(9) Récemment, à propos d'un avant-projet de loi sur la télématique médicale, le Ministre de la Santé publique a proposé la création pour le secteur de la santé et ses applications d'un identifiant séparé et ce afin de cloisonner les traitements de données de santé des autres traitements. L'avant-projet présenté sur le site du Ministère de la santé publique : http://www.health.fgov.be a malheureusement été retiré.

(10) Cf. l'article 13 de l'avant projet de loi relatif à certains traitements de données à caractère personnel par le Service public fédéral Finances soumis en première lecture à la Commission belge de protection de la vie privée (Avis n° 01/2007 du 17 janvier 2007) et au Conseil d'Etat. A ce propos, on s'étonne de la remarque de la Commission à propos de l'avant projet : «*La Commission estime que la création d'un numéro spécifique et son imposition à des utilisateurs externes créeront en effet un 2ème numéro universel en surplus du numéro de registre national ce qui risque d'entraver le niveau de protection de la vie privée dans la mesure où il sera repris dans plusieurs banques de données externes au SPF Finances et où la nécessité de conversion impliquerait des risques d'erreur sur l'identification...*».

(11) Loi du 16 janvier 2003 portant création d'une Banque Carrefour des entreprises, modernisation du registre du commerce, création de guichets-entreprises, agréées et portant diverses dispositions, *M.B.*, 5 fév. 2003. Le fonctionnement de cette Banque Carrefour repose sur la création d'un identifiant «Entreprises». Sur la Banque carrefour des entreprises, la notion large d'entreprise et les données disponibles auprès de ce registre central, lire P. EVRARD, M. GODIN, «La Banque-Carrefour des Entreprises», in *La Revue du Barreau de Liège, Actualités*, disponible in : http://liege.obfg.be/revue/actualité_080104_carrefour.htm.

vernement s'apprête à créer un identifiant unique des biens immobiliers.

2. – *Les sources dites «authentiques»*

7. La création du registre national est également considérée comme préfiguratrice du développement de la notion de «source authentique».

En réalité, outre le numéro dont il a déjà été question, le registre reprend, hier, neuf, aujourd'hui, treize informations de base sur chaque citoyen, informations soigneusement vérifiées et mises à jour par les communes via un portail changement d'adresse.

Chaque administration dont la fonction nécessite une de ces informations, peut l'obtenir auprès du registre national sans devoir la collecter de la personne concernée.

La notion de «source authentique» est aujourd'hui consacrée en Belgique. Le fonctionnement des administrations électroniques reliées entre elles au sein d'un vaste réseau, nécessite de manière accrue le partage d'informations entre administrations au sein de ce réseau et souligne l'importance d'une information de qualité, disponible auprès de sources dites «authentiques» (12). L'article 7 de l'accord de coopération du 23 mars 2001 (13), sur lequel nous reviendrons, définit cette notion de la manière suivante : «*En concertation avec les parties, les tâches seront progressivement réparties en tenant compte de la répartition des compétences, en vue d'offrir un accès aux données stockées sous forme authentique. Chaque catégorie de données se verra attribuer un service administratif dépositaire chargé d'en assurer le stockage et la mise à jour en tenant compte autant que possible des besoins de tous les autres services administratifs*». En d'autres termes, pourquoi collecter cent fois la même information auprès des citoyens alors que celle-ci peut être

(12) «Pour veiller à ce que les données déjà disponibles dans une administration ne soient plus redemandées à chaque fois, a été introduit le principe des «sources authentiques». Cela signifie que l'administration qui, fonctionnellement parlant, traite le plus une série de données, est désignée comme la seule responsable de la demande et de la mise à jour des données. D'autres administrations qui ont besoin de ces données doivent dès lors pouvoir les utiliser. Cela se fait en utilisant d'autres fondements comme des clés d'identification unique et l'Universal Messaging Engine. Pour protéger au maximum la vie privée, cet échange de données doit toujours se fonder sur une base légale et conformément aux principes de finalité et de proportionnalité. Une sous-commission de la Commission pour la protection de la vie privée contrôle l'ensemble du processus.» (Extrait de la note sur le e-Government disponible sur le site de FEDICT déjà cité).

(13) *M.B.*, 8 août 2001.

trouvée par l'ensemble des autorités administratives auprès d'une administration unique, chargée d'en garantir la fiabilité et de la fournir à l'ensemble des autres administrations ? Ainsi, se sont multipliées les intronisations légales de sources : la documentation patrimoniale (STIPAD) au sein du Ministère des Finances, la Banque carrefour des Entreprises, etc.

Au-delà des administrations, certaines fédérations privées, celles de notaires, des huissiers, des avocats se voient appeler à devenir également «sources authentiques» authentifiant la qualité de leurs membres auprès des administrations, ainsi celles fiscales et judiciaires (14).

8. Au-delà, s'affirme progressivement le 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 habilitées 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, auprès de l'administration de la population, la composition du ménage, auprès de l'administration de la sécurité sociale, directement les données de revenus, auprès de la Banque carrefour des entreprises, les différentes fonctions exercées par le contribuable comme dirigeant ou administrateur d'entreprise, etc. ? Sans doute, l'efficacité adminis-

(14) Ainsi, dans le cadre du projet Phénix qni crée un système d'information de l'ensemble du secteur judiciaire. Loi du 10 août 2005 instituant le système d'information Phénix, *M.B.*, 1er septembre 2005. Sur cette loi, lire J.F. Henrotte (éd.), *Phénix et la procédure électronique*, CUP-Larcier, 02/2006, Vol. 85.

trative y trouve son compte! Par contre, le citoyen s'inquiète à juste titre de l'absence 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 du fait 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.

9. 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 j'ai bien compris la portée de certains articles du décret de décembre 2005 qui instaurent au profit du citoyen ce droit alternatif. 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 (15).

(15) Voire participer au développement et au design des systèmes d'information du gouvernement électronique, sur ce point, parlant de la tradition scandinave, A. JANSEN, «User involvement in E-Government System Development Projects : What can be learned from the past!», *Yulex*, 2006, pp. 65 et s. D.W. SCHARTUM,...

3. – *De la signature électronique aux transactions électroniques*

10. L'utilisation des systèmes d'information mis en place par les agents des services publics tout comme les transactions électroniques, que les citoyens entendent passer avec l'administration, nécessitent des outils électroniques d'authentification voire de signature.

C'est dans ce contexte que, par une loi de janvier 2003, le gouvernement belge a imposé à chacun la carte d'identité électronique comme outil d'authentification et l'a doublé d'une possibilité de signature électronique. Chaque fois qu'un agent souhaitera accéder à un traitement, il pourra grâce à sa carte d'identité et un code secret s'authentifier (16), si le citoyen souhaite passer une transaction électronique avec l'administration, la carte d'identité et la signature électronique remplaceront avantageusement la signature manuscrite et permettront de résoudre les questions soulevées par Mr. Ferraci, lors de son intervention à propos de l'absence de sécurité des transactions électroniques passées avec l'Administration.

Sans doute, nonobstant les facilités que la transaction électronique offre au bénéfice tant du citoyen que de l'administration, on veillera à ne pas obliger les usagers de l'administration à communiquer ou poser des actes vis-à-vis de l'administration uniquement par voie électronique. Cela serait en effet contraire au principe d'égalité et de non-discrimination. On note en ce sens, l'article 4, §1er de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (17) : ***«A défaut de dispositions légales contraires, nul ne peut être contraint de poser un acte juridique par voie électronique.»***

11. Demain, la carte d'identité électronique et sa signature pourraient être utilisées également pour les achats sur Internet, pour sécuriser l'accès à certains endroits, pour loger la carte de crédit, etc. Reste à installer les lecteurs et à convaincre le marché de son intérêt mais Bill Gates en visite, l'année dernière, à Bruxelles, ne se

(16) Outre que pour des raisons de sécurité, cette authentification sera liée à un profil d'accès qui permet de vérifier de manière automatique dans quelle mesure l'agent du service public ou de manière plus générale la personne qui sollicite l'accès, peut avoir accès en raison de ses fonctions à telle ou telle donnée, à tel ou tel traitement.

(17) *M.B.*, 29 septembre 2001.

disait-il pas pleinement convaincu de l'intérêt pour le marché de cette carte et de la signature qu'elle permet de générer?

Ainsi, ce bout de papier à la dimension symbolique lourde qui était réservé hier, à l'identification vis-à-vis de l'autorité policière deviendrait le sésame universel, celui dont la perte vous raye du monde civilisé.

Progressivement, les critiques se font bruyantes à l'encontre de la généralisation de l'usage de cet outil. Ne faut-il pas distinguer les outils d'authentification et de signature suivant les contextes: signer comme citoyen n'est pas signer comme médecin, ni comme consommateur intéressé par le site d'Amazon? Ne faut-il pas réserver la carte d'identité aux seules applications administratives et la limiter à un contenu minimum?

12. Les transactions avec l'administration sont marquées par un formalisme parfois désuets (les biffures et ratures en marge) mais souvent plein de bon sens et de respect de l'intérêt des contribuables.

L'électronique risque de les mettre à mal. Ce défi peut être rencontré par le principe de l'équivalent fonctionnel, comme il est suggéré par une récente étude. Ce principe, déjà affirmé pour légitimer la signature et l'écrit électronique exige que l'administration se dote d'outils technologiques capables d'assurer le respect des fonctionnalités essentielles qui justifiaient le formalisme papier (18). La région Wallonne a dernièrement pris en ce sens un décret (19) consacrant ce principe. Son article unique dispose : «*Un formulaire électronique de la Région wallonne complété, validé et transmis, avec ses éventuelles annexes, conformément aux modalités et conditions définies par le Gouvernement, est assimilé au formulaire papier portant le même intitulé, complété, signé et transmis, avec ses éventuelles annexes, à l'administration concernée, conformément aux dispositions décrétales et réglementaires.*».

(18) L'approche dite de l'équivalence fonctionnelle repose alors sur une analyse des objectifs et des fonctions de l'exigence légale de forme, que l'administration impose. Cette analyse faite, il s'agit de rechercher tout en respectant la neutralité technologique les moyens électroniques qui permettent d'assurer l'accomplissement de ces objectifs (Sur cette théorie, son intérêt et sa consécration en droit belge par l'article 16 de la loi du 11 mars 2003, lire entre autres : M. DEMOULIN et E. MONTERO, «La conclusion des contrats par voie électronique», *in* M. FONTAINE (sous la direction de), *Le processus de formation du contrat. Contributions comparatives et interdisciplinaires à l'harmonisation droit européen*, Bruxelles, Bruylant et Paris, L.G.D.J., 2002, p. 716, n° 32. Pour plus de développements sur la théorie des équivalents fonctionnels, voy. D. GOBERT et E. MONTERO, «La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle», *D.A./O.R.*, 2000, n° 53, pp. 17- 39. Une étude récente du CRID signale pas moins de onze catégories d'exigences formelles présentes dans les formulaires ou documents de l'administration.

(19) *M.B.* 27 décembre 2006, p. 74735. Cf également l'exposé des motifs (Parlement Wallon, Session 2006-2007, 6 oct. 2006, *Doc.* 467 (2006-2007), n° 1.

Au niveau fédéral, on note que le Conseil des Ministres a récemment créé une «Charte à destination de l'administration» intitulée : «*Charte pour une administration à l'écoute des usagers*». Cette Charte (20) établit des principes similaires à celui de l'«équivalent fonctionnel», adopté en Région Wallonne mais sans avoir d'autre portée qu'un encouragement à l'utilisation de procédés électroniques entre administrations et citoyens (21).

II. – DE LA BANQUE-CARREFOUR DE LA SÉCURITÉ SOCIALE AUX COMITÉS SECTORIELS ET AUX QUESTIONS POSÉES PAR LA STRUCTURE FÉDÉRALE DE LA BELGIQUE

Telle que modifiée par la loi du 26 février 2003.

1. – *Les réseaux sectoriels dans l'administration fédérale*

13. Evoquons le second précédent mentionné lors de notre introduction : la Banque-carrefour de sécurité sociale (en abrégé : BCSS) qui, fondée en 1990 (22), 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 (ils sont plus de 50) et, à la fois, comme un outil de contrôle des communications entre le secteur de la sécurité sociale et le reste des administrations.

(20) Cette Charte devrait bientôt être coulée dans les formes d'une circulaire et publiée au *Moniteur Belge*. Voyez http://www.belginm.be/eportal/application?pageid=contentPage&docId=42763, Conseil des Ministres du 23 juin 2006, Améliorer le service au client : l'administration s'engage. Insistons sur le fait que cette charte est créée par l'exécutif à destination des seules administrations fédérales.

(21) Certains points de la charte mériteraient d'être développés. Ainsi, le point 9 : «*9. Tout service public répondra aux courriers électroniques et aux lettres en empruntant les mêmes voies, à moins que les données soient de nature à déconseiller toute communication électronique [...].*»... «*Si un service public est contacté pour information ou pour une demande par voie électronique (conformément aux points 6 et 7), il sera dans l'obligation de répondre via le même mode de communication sauf si les données sont de nature à déconseiller toute communication électronique*».

(22) Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque Carrefour de la sécurité sociale (*M.B.*, 22 février 1990).

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 dans son excellent écrit.

Ce précédent fait aujourd'hui recette. Se multiplient les réseaux sectoriels, celui de la justice (Phénix) (23), celui de la santé (Be-Health) (24) celui de l'économie et de l'emploi (la Banque-carrefour des entreprises (BCE)) (25), celui pressenti des Finances (COPER-FIN) (26). 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 risques (27), etc.

(23) Loi du 10 août 2005 instituant le système d'information Phénix (*M.B.*, 1er sept. 2005) : article 1 «*Il est créé un système d'information appelé Phenix, qui a pour finalités, la communication interne et externe requise par le fonctionnement de la Justice, la gestion et la conservation des décisions judiciaires, l'instauration d'un rôle national, la constitution d'une banque de données de jurisprudence, l'élaboration de statistiques et l'aide à la gestion et l'administration des institutions judiciaires.*».

(24) Avant-projet de loi sur la télématique médicale disponible sur le site du Ministre de la santé publique, sur cet avant projet, lire Y. POULLET, «E-Health – A legislative approach : the Belgian Case», in *Proceedings of the seminar held by the CRID at the XXXVth colloquium on Medical law*, Toulouse, 10th of Augustus, à paraître, Fondation Brochet, 2007.

(25) Loi portant création d'une Banque-carrefour des entreprises (BCE), modernisation du registre du commerce, création de guichets entreprises agréés et portant diverses dispositions, *M.B.*, 5 février 2003. A noter l'article 3 : «*Ce registre (la BCE) associé à l'introduction d'un numéro unique d'entreprise a pour objectif, en application du principe de la collecte unique de données de permettre de simplifier les procédures administratives s'adressant aux entreprises ainsi que de contribuer à l'organisation plus efficace des services publics.*»

(26) Avant projet de loi relatif à certains traitements de données à caractère personnel par le Service Public fédéral Finances déjà cité.

(27) «*Par gestion de risques, on entend les traitements appliquées à des données à caractère personnel codées ou non ou à des données anonymes et mises en place pour identifier les risques et groupes de risques, d'objets et de sujets liés au non respect total ou partiel des dispositions légales et réglementaires dont l'exécution est assurée par le Service Public Fédéral.*» (Art. 16 de l'avant projet de loi relatif à certains traitements de données à caractère personnel par le Service Public fédéral Finances, déjà cité).

2. – *Les Comités sectoriels*

14. L'article 31*bis* de la loi de 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 (28), de la Banque carrefour des entreprises (29), de l'autorité fédérale (30) et le comité de surveillance dans le secteur judiciaire dans le cadre du projet Phénix (31). S'ajouteront sans doute, des comités de surveillance en matière de télématique médicale (32), en matières statistiques et fiscales (33), etc. (34). On ajoutera que l'article 36*bis* de la loi du 8 décembre 1992 (35) institue au sein de la Commission pour 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.*».

15. 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

(28) Loi du 25 mars 2003, art. 12 (*M.B.*, 28 mars 2003).

(29) Art. 27 de la loi du 16 janvier 2003.

(30) ... créé par l'article 36*bis* de la loi du 8 décembre 1992 telle que modifiée par la loi du 26 février 2003.

(31) Il s'agit du comité de surveillance sectoriel Phénix créé par la loi du 10 août 2005 instituant le système d'information Phénix (*M.B.*, 1er sept. 2005).

(32) .Un sous comité «sectoriel» Santé a été créé par la loi programme du... au sein du Comité surveillance de la Banque-carrefour de sécurité sociale.

(33) Avant projet de loi relatif à certains traitements de données à caractère personnel par le Service Public Fédéral (SPF) Finances, approuvé par le Conseil des Ministres du 22 décembre 2006 et actuellement soumis à l'avis du Conseil d' Etat. En l'occurrence, il s'agit plus d'un Comité interne au SPF Finances avec présence d'experts que d'un Comité sectoriel créé au sein de la CPVP.

(34) On pourrait également songer en outre à des comités sectoriels au niveau régional et communautaire voire locaux

(35)

en ce qui concerne les flux relevant de sa compétence (36). Le droit de recours des destinataires suite à une décision négative des comités sectoriels 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 (37).

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.

16. On relèvera avec D. de Bot (38) qu'il est cependant à craindre que cette proximité du terrain est renforcée par le fait que chaque comité est «flanquée» d'une institution de gestion du secteur concerné, qui prépare l'avis technique et juridique relatif au dossier introduit par cette dernière (39). L'intervention de ces institutions favorise en définitive une plus grande complicité avec les administrations chargées par ailleurs d'instruire le dossier et que le comité a pour compétence de contrôler. 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 compé-

(36) Pour rappel, le comité sectoriel «*pour l'autorité fédérale*» de l'article 36*bis* déjà cité contrôle de toute façon tous les flux antre autorités publiques qui ne sont pas soumis à la compétence d'un comité sectoriel créé en vertu d'une loi particulière.

(37) E. Degrave, «La Commission de la protection de la vie privée : un organisme invincible?», *R.T.D.I.*, 2006, pp. 237-238. En effet, même si ces comités sectoriels – dans la mesnre de l'exercice de leurs ponvoirs de décision – constituent des «autorités», dès lors que «*leur fonctionnement est déterminé et contrôlé par les pouvoirs publics et qu'elles peuvent prendre des décisions obligatoires à l'égard des tiers...*» (Snr ces critères, lire D. De Roy, «Etre ou ne pas être une autorité administrative», *Droit communal*, 2002/2, pp. 200 et s. et F. Vandendriessche, «De invulling van het begrip administratieve overheid na de arresten Gimvindus en BATC van het hof van Cassatie», *R.W.*, 2000, pp. 497 et s.), la proximité de la Commission de protectiou de la vie privée (au sein de laqnelle sont instituées ces comités sectoriels) avec la Chambre des représentants, organe du pouvoir législatif, pourrait exclure, dans le chef de ces comités, toute reconnaissance de la qualité d' «autorité administrative» (au sens de l'art. 14, al. 1er, des lois coordonnées sur le Conseil d'Etat) conditionnant la compétence d'annulation dn Conseil d'Etat.

(38) D. De Bot, «De Commissie voor de Bescherming van de Persoonlijke Levensfeer : Tussen droom en daad bestaaan er niet alleen wetten in de weg, maar vooral praktische problemen», *RGDC*, 2003, pp. 384 et s. Cf. également nos réflexions critiques in Y. Poullet, «L'autorité de contrôle : vues de Bruxelles», *Revue Française d'administration publique*, n° spécial, 1999, pp. 69 et s.

(39) Cf. article 31*bis*, §3 de la loi du 8 décembre 1992, introduit par l'article 6 de la loi du 26 février 2003 (*M.B.*, 26 juin 2003).

tences 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 (l'équivalent de la CNIL) mais son fonctionnement le rapproche du terrain à contrôler, et ce au risque d'un affaiblissement des principes de la protection des données.

3. – *Quid de la coopération entre les administrations relevant des différents niveaux de pouvoirs dans une Belgique fédérale?*

17. Pour ceux qui voient la Belgique comme un pays en voie d'extinction ou du moins d'éclatement, je terminerai en disant que la technologie et les systèmes modernes d'information peuvent sans doute constituer un outil fort de dialogue et de compréhension mutuelle, entre les différentes composantes de mon pays.

Dès 2001, les gouvernements fédéral des 3 Régions, des 3 Communautés signaient un accord de coopération (40) pour la mise sur pied d'une «*plate-forme électronique permettant une communication rapide et directe aussi bien entre l'autorité et les citoyens, entreprises*

(40) Accord interinstitutionnel du 23 mars 2001 entre l'Etat fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Régiou de Bruxelles-capitale, la Commission communautaire flamande, la Commission communautaire française et la Commission communautaire commune concernant la construction et l'exploitation d'une e-plate forme commune (*M.B.*, 8 août 2001). A noter depuis, un second accord et surtout la Résolution snr l'e-government intégré en exécution du 2ème accord de coopération intergouvernemental en matière d'e-government décidée à l'occasion du Congrès sur l'e-government à Bruxelles des 7 et 8 novembre 2006.

et autres organisations, qu'entre les parties elles-mêmes». Ils s'entendaient sur une infrastructure commune, un site portail fédérateur, des normes de transmission et de structures des messages communs. En outre, les parties contractantes s'engageaient à partager les mêmes sources authentiques et à développer des «**Best Practices**». Belle occasion de permettre à toutes les administrations depuis la commune jusqu'à l'état fédéral de développer un e-government à la belge.

18. Comme l'Etat fédéral a créé son service en charge des technologies : le FEDICT (41), chacune des Régions a développé son propre service de conception et d'aide à la réalisation de l'e-gouvernement. Ainsi, la Région Wallonne a crée sa propre structure de coordination : easi-wal (42), de même que la Région flamande avec le CORV@ (Coordinatiecel Vlaams e-government) (43). Ces structures régionales développent des stratégies autonomes et disposent souvent de priorités propres, ce qui ne facilite pas nécessairement la coordination des politiques entre les niveaux régionaux et fédéral. Pour remédier à cela, le nouvel accord interinstitutionnelle de coopération prévoit d'institutionnaliser une concertation plus systématique entre les organismes en charge de la question aux différents niveaux de pouvoir. Sans doute cette concertation permanente permettra une meilleure intégration des politiques et la définition de stratégies communes dans le développement des applications mais on peut en douter si le leadership de l'autorité fédérale n'est pas reconnu à travers les impulsions de FEDICT.

(41) www.fedict.be.

(42) http://www.easi-wal.be. Les missions du Commissariat sont les suivantes :

- la coordination générale et transversale des actions menées par le Gouvernement wallon en matière de simplification administrative, d'informatisation des processus et d'E-gouvernement,
- la direction et la gestion quotidienne du Commissariat, de ses ressources en personnel, de ses ressources budgétaires et des moyens matériels mis à sa disposition,
- l'exploration de toutes les opportunités de simplification et d'informatisation des procédures, d'amélioration de la lisibilité des textes dans un souci de qualité du service et de l'information vers les usagers,
- l'évaluation permanente de l'avancement des projets de manière à faire rapport au Gouvernement wallon et à informer les responsables administratifs concernés de leur mise en oeuvre au sein des services.

(43) http://www3.vlaanderen.be/e-government/. Le Corv@ dispose de compétences similaires à celle d'Easi-wal.

En guise de conclusions

19. Peut-on parler d'un modèle belge ? Sans doute plus que d'autres pays, la Belgique a développé une politique volontariste de développement de l'e-gouvernement. Le paysage, que nous avons décrit, est marqué par des choix dont certains de longue date, choix que certains pays voisins peuvent nous envier : le numéro de registre national comme clé d'identification unique, la constitution de réseaux sectoriels, le principe du guichet et de la collecte unique, la carte d'identité électronique à laquelle couplée une signature électronique officielle. Ces choix facilitent indéniablement le développement d'un back office efficace sur lequel pourront s'appuyer des applications citoyennes ou en direction des entreprises ou autres organisations privées.

Sans doute, ces choix volontaristes, dictés souvent par une idéologie technicienne au seul service de l'efficacité administrative, souffrent d'un déficit de discussions démocratiques, ils inquiètent les défenseurs des libertés. Les développements conduits par une approche sectorielle et régionale laissent mal deviner une stratégie plus globale et sans nul doute empêchent la formulation de principes législatifs généraux qui devraient régir l'ensemble de nos administrations : on regrette que des principes de non discrimination (obligation de conserver des procédures traditionnelles, possibilité de choix de la manière dont les citoyens peuvent ou non déléguer à l'administration le soin de rechercher elle-même les données), de proportionnalité (réserver aux citoyens une part des bénéfices d'efficacité dégagés par l'utilisation des technologies de l'information et de la communication), de transparence (suivi des dossiers en ligne, transparence complète des sources d'information utilisés), d'équivalence fonctionnelle ne soient pas proclamés.