INTRODUCTION - LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ET L'E-GOUVERNEMENT

Cécile DE TERWANGNE
Professeur à la Faculté de Droit de l'Université de Namur (FUNDP) – Belgique
Directrice de l'Unité « Société de l'information et libertés »
du Centre de Recherches Informatique et Droit (CRID)

I. DESCRIPTION DE L'ADMINISTRATION EN LIGNE

L'administration électronique ou en ligne, communément appelée e-gouvernement, consiste en l'utilisation par le secteur public des technologies de l'information et de la communication (TIC) pour l'accomplissement des missions qui lui incombent (1). Nos gouvernements ont été rapidement séduits par les perspectives offertes par le déploiement de l'e-gouvernement. En effet, le recours aux TIC permet de rationaliser le fonctionnement des administrations et de se doter d'outils de gestion publique performants (*back office*). Mais l'administration dispose aussi désormais d'un instrument de simplification de la relation avec le citoyen et l'entreprise, et d'un outil de communication d'informations au public (*front office*). L'introduction des technologies de réseau au sein du monde administratif s'accompagne donc de bouleversements tant internes qu'externes. Ces bouleversements ont peu à peu débouché sur la réorganisation et la modernisation des services classiques mais également sur l'apparition de nouveaux services.

II. CHANGEMENT DE PARADIGME : DE L'ADMINISTRATION EN SILO À L'ADMINISTRATION EN RÉSEAU

Traditionnellement, les administrations publiques sont structurées en silos cloisonnés, indépendants les uns des autres. Ce modèle en silos signifie que chaque entité se voit attribuer des missions et compéten-

(1) Dans sa Communication du 26 septembre 2003 sur Le rôle de l'administration en ligne (e-Government) pour l'avenir de l'Europe, la Commission européenne définit l'e-Government comme « l'utilisation des technologies de l'information et des communications (TIC) dans les administrations publiques, associé à des changements de l'organisation et de nouvelles aptitudes afin d'améliorer les services publics et les processus démocratiques, et de renforcer le soutien des politiques publiques.» (Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions, COM(2003) 567 final, p. 8.

ces bien définies pour la réalisation desquelles elle dispose d'informations qui lui sont propres. Chaque administration instaure en outre ses propres processus de traitement de ses informations. Ce modèle conduit à la mise en place de systèmes d'information verticaux et fermés. Dans un tel contexte, la communication des informations entre entités publiques, de même que le partage des données, sont particulièrement limités. Là où ils sont autorisés, communication et partage des informations sont encadrés par des réglementations strictes. Quant au transfert de données hors du secteur public vers des partenaires privés, il est encore plus sévèrement restreint.

Ce modèle que l'on peut qualifier de « vertical » était jusqu'il y a peu encore, présenté comme la garantie contre un État omniscient à l'égard duquel le citoyen serait totalement transparent (2).

Le développement de l'administration électronique ou de l'e-gouvernement s'est accompagné de l'abandon progressif du modèle en silo au profit d'un modèle d'administration en réseau. Reliées entre elles par un réseau électronique performant, les autorités publiques sont désormais à même de communiquer tant entre elles qu'avec l'extérieur.

Ce renoncement à la garantie traditionnelle contre Big Brother doit être considéré avec lucidité et non avec la certitude béate que le progrès technique est bon en soi. Certes, il ne s'agit pas de tourner le dos aux technologies nouvelles et à leurs formidables performances, mais il ne faut pas le payer à n'importe quel prix. On ne peut réduire l'État à un simple fournisseur de services en quête d'efficacité. L'efficacité est assurément une valeur à promouvoir au sein des administrations publiques. Cependant, étant donné la quantité et la nature des données à caractère personnel traitées par le secteur public, et le caractère obligatoire de leur collecte, d'autres valeurs doivent impérativement être également prises en considération.

De nombreux projets de développement de l'administration électronique mettent directement en cause l'équilibre à trouver entre fonctionnement efficace de l'administration et intérêts des administrés, notamment la maîtrise par ceux-ci des informations qui les concernent. Un scrupuleux respect des législations de protection des données à caractère personnel devrait permettre de répondre à ce souci d'équilibre. Dans les paragraphes qui suivent, on relève les implica-

(2) D. DE ROY, C. DE TERWANGNE, Y. POULLET, « La Convention européenne des droits de l'homme en filigrane de l'administration électronique », in *50 ans d'application de la CEDH en Belgique : entre ombres et lumières*, Actes du Colloque organisé par le Centre de droit public de l'ULB les 20 et 21 octobre 2005 à Bruxelles, à paraître.

tions de la protection des données personnelles dans des développements majeurs de l'e-gouvernement.

III. Principe de collecte unique des données et protection des données

Une des préoccupations affichées des promoteurs de l'e-gouvernement est de viser à organiser le fonctionnement de l'administration de manière à éviter les demandes répétées des mêmes informations auprès des citoyens ou des entreprises. C'est le principe de collecte unique des données. La réponse à cette préoccupation implique nécessairement un partage d'informations entre les entités publiques intéressées. Il s'impose de favoriser la solution technique qui maintient les données auprès de l'autorité publique qui les a récoltées en premier (3) et de permettre aux autres autorités d'accéder aux données (4), plutôt que de créer une nouvelle base de données communément accessible, rassemblant l'ensemble des données collectées par les différentes autorités publiques (5).

Le point crucial dans ce cas est celui de la réglementation de l'accès aux données. Il convient de déterminer avec précision qui peut accéder à quoi (et qui détient ce quoi). C'est l'application du principe de finalité qui permettra de déterminer cela : une autorité publique pourra accéder aux données seulement dans la mesure où c'est nécessaire pour accomplir ses tâches et répondre à ses obligations légales. Par ailleurs, l'autorité publique ne pourra accéder qu'aux données pertinentes, adéquates et non excessives au regard de la finalité pour laquelle elle souhaite accéder aux données. En outre, les citoyens doivent être informés de cette mise en place d'un accès partagé aux données.

---

(3) Ou auprès de l'autorité publique désignée comme source authentique de cette catégorie de données. Sur ce modèle, voy. en Belgique la Banque-carrefour des entreprises : un arrêté royal désigne les autorités, administrations et services qui sont chargés de la collecte unique et de la tenue à jour des données relatives à toutes les personnes morales du pays (Loi du 16 janvier 2003 portant création d'une Banque-carrefour des entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions, *M.B.*, 5 février 2003, accessible à l'adresse http://www.cass.be/loi/loi.htm).

(4) En Belgique, l'article 22 de la loi sur la Banque-carrefour des entreprises qui instaure le « principe de la collecte unique de données » interdit aux autorités autorisées à consulter cette banque de données de réclamer encore les mêmes données aux personnes concernées.

(5) Voy. l'exemple belge de la Banque-carrefour de la sécurité sociale (http://kszbcss.fgov.be/fr/index.asp), récompensé par l'ONU qui lui a décerné un « Public Service Award » le 23 juin 2006. Le système crée un processus de traitement automatisé entre près de 2.000 institutions. En 2005, environ un demi-milliard de messages électroniques ont été échangés.

IV. GUICHET UNIQUE ET PROTECTION DES DONNÉES

Le développement de points d'entrée unique suscite le même souci lié au partage des données entre administrations.

De nouveaux services ont vu le jour avec le déploiement de l'e-gouvernement, orientés autour d'« événements de vie » ou d'« épisodes professionnels ». La Commission européenne a éclairé le sens de l'expression 'événement de vie' : « The term 'life events' refers to the government services needed at specific stages in life » (6). À titre d'exemples d'événements de vie autour desquels on organise désormais l'offre des services administratifs, on peut citer la naissance d'un enfant, le démarrage ou la fin d'un parcours scolaire, le mariage, le changement de statut professionnel, le déménagement, le départ à la retraite, etc. Quant aux 'épisodes professionnels', ils correspondent, d'après la Commission, aux événements intervenant dans le cycle de vie d'une entreprise : « The term 'business episodes' refers to the components of the business life cycle » (7). Il s'agit par exemple du fait de démarrer une entreprise, d'engager du personnel, d'acquérir une licence ou une autorisation, de payer les impôts et taxes, de vendre la société ou de la transmettre, etc.

L'idée est donc de permettre aux citoyens ou aux entreprises de trouver, à un point d'entrée unique, l'ensemble des informations en lien avec l'événement qui les concerne. L'ensemble des démarches est donc regroupé à ce point d'entrée unique.

L'offre de tels services nécessite le rassemblement d'informations détenues par différents départements administratifs. Ici à nouveau, comme pour le principe de collecte unique des données, les mêmes questions de respect des finalités des traitements des données et d'accès limité aux données pertinentes doivent être prises en compte.

V. INTEROPÉRABILITÉ

Le phénomène du partage d'informations ramène à la question très à la mode de l'interopérabilité.

---

(6) European Commission, « Linking up Europe : the importance of Interoperability for e-Government services », Commission Staff Working paper, IDA publications, January 2004, available at http://europa.eu.int/idabc/en/document/2036/5583. Un exemple de ce nouveau type d'organisation de l'information mise à disposition du public peut être trouvé sur le portail de l'administration française 'Service-Public.fr' accessible à l'adresse http://www.servicepublic.fr/

(7) European Commission, *ibidem*. Un exemple de services d'e-gouvernement basés sur les épisodes professionnels peut être trouvé sur le site web du gouvernement irlandais 'Basis - Business Access to State Information and Services' http://www.basis.ie.

« Interoperability means the ability of information and communication technology (ICT) systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge » (8). Le terme d'« interopérabilité » vise non seulement l'utilisation en commun de systèmes d'information à grande échelle, mais également les possibilités d'accès aux données, d'échange de données et de fusion de bases de données.

Ainsi que l'a souligné le Contrôleur européen à la protection des données, on ne peut réduire la question de l'interopérabilité à une question technique. « En effet, il est évident que rendre techniquement possible l'accès à des données ou leur échange constitue, dans de nombreux cas, une puissante incitation à y accéder *de facto* ou à les échanger. On peut donc, sans trop s'avancer, partir du principe que les moyens techniques seront utilisés dès qu'ils seront disponibles. » (9).

Aborder la question de l'interopérabilité ne peut donc se faire sans réfléchir à la légitimité du partage de données qui en découlera. On doit veiller au respect du principe de proportionnalité : l'atteinte qu'un accès élargi aux données et une possibilité plus grande d'utilisation de ces données représente pour les personnes concernées ne doit pas être supérieure à l'intérêt lié au partage des données en question. Une juste proportionnalité doit exister entre intérêts des sujets des données et intérêts des utilisateurs de celles-ci.

Le principe de finalité doit de même, une fois encore, être respecté : on ne peut faire avec les données que ce qui est compatible au regard des finalités poursuivies au départ. En outre, la transparence doit régner sur les opérations rendues possibles grâce à l'interopérabilité et sur les départements interconnectés.

VI. Transparence des flux et des accès aux données

La transparence est au demeurant une exigence essentielle accompagnant le déploiement de l'administration en ligne. L'exigence de transparence spécifique à l'e-gouvernement est double. Il faut garantir la transparence des flux de données (quels sont les flux de données instaurés, entre quelles administrations, dans quelles circonstances) et la transparence des accès aux données (qui a accès à telles ou telles données, dans quel but). Dans un monde administratif en réseau, il est

(8) European Commission, «European Interoperability Framework for pan-European e-Government Services», version 1.0, November 2004, http://europa.eu.int/ida.bc/en/document/3473/6886.

(9) Contrôleur européen à la protection des données, Commentaires sur la Communication de la Commission sur l'interopérabilité des bases de données européennes, 10 mars 2006, disponible à l'adresse www.edps.eu.int.

impératif de mettre en place des moyens techniques et organisationnels pour empêcher les accès non autorisés. La conservation des traces laissées par les fonctionnaires accédant aux données permet de contrôler le respect des limitations d'accès instaurées.

VII. MOYENS D'IDENTIFICATION : CARTE D'IDENTITÉ ÉLECTRONIQUE ET NUMÉRO D'IDENTIFICATION UNIQUE

On terminera ce propos en évoquant encore deux instruments phares de l'e-gouvernement.

Le premier est la carte d'identité électronique. C'est généralement avec fierté et persuadés d'un impact électoral positif que les gouvernements annoncent l'instauration de la carte d'identité électronique. La présentation de cet outil d'identification électronique infaillible, véritable sésame pour un ensemble toujours plus grand de services administratifs en ligne, se fait sur un ton enthousiaste, prometteur d'efficacité. Il est clair qu'il s'agit d'une avancée qui permet aux administrés de recourir effectivement aux nouveaux services mis en place. Mais elle ne doit pas se réaliser sans réflexion sur les enjeux qu'elle suscite pour la vie privée et le rapport de l'individu à la société. Si la technique se révèle au point, cette carte aura vite tendance à être utilisée comme moyen systématique d'identification des personnes en ligne. Il importe dans ces circonstances de bien peser ce que l'on décide de faire apparaître sur la carte. Il est aussi essentiel que l'on n'associe pas trop de fonctions ou que l'on n'intègre pas trop de dossiers sur cette carte. Est-il opportun, par exemple, de joindre un outil de paiement à la carte ? Une telle association fera de la carte un inquiétant moyen de surveillance des citoyens, permettant de suivre et enregistrer toutes les traces électroniques laissées par l'utilisation de la carte. Des dossiers tels le dossier médical ne doivent pas non plus figurer sur la carte d'identité électronique, étant donné le risque, jamais totalement absent, que des personnes non autorisées y accèdent.

Le rassemblement de trop de fonctions et de fichiers sur un même instrument identifiant est source de danger pour la vie privée des individus, étant donné la concentration des traces liées à une utilisation multiple et le risque de perte de confidentialité des données stockées et d'accès non autorisés.

Le deuxième instrument est le numéro d'identification unique. L'attribution d'un « numéro national » à chaque citoyen depuis sa naissance n'est pas une nouveauté apparue avec les TIC. Des États recouraient déjà auparavant à cet instrument d'identification et de gestion administrative. L'utilisation d'un numéro identifiant unique était le plus souvent encadrée de manière stricte. La mise en réseau des

différents départements administratifs, l'interconnexion électronique des services créent toutefois un environnement dans lequel l'utilisation d'un numéro d'identification unique a une portée bien plus large. Dans le contexte de l'administration en ligne, le recours à un outil d'accès transversal aux données d'un individu présente un danger plus grand pour celui-ci du fait des croisements d'informations rendus possibles. Les États doivent veiller à instaurer des numéros d'identification distincts, spécialement dans les domaines comme la sécurité sociale ou l'administration fiscale qui brassent de grandes quantités de données sensibles et intimes.

S'il faut en résumé saluer le développement de l'administration électronique porteuse des promesses d'efficacité et de performance de la technique, on invite les gouvernements à prendre scrupuleusement en considération les enjeux qu'un tel développement présente pour les droits des citoyens, spécialement leur vie privée et leur maîtrise des données qui les concernent.