L'e-gouvernement et la protection de la vie privée

Degrave, Elise

Published in:
Chroniques de droit public - Publiekrechtelijke kronieken

Publication date:
2013

Document Version
le PDF de l'éditeur

L'e-gouvernement et la protection de la vie privée

Elise DEGRAVE
Maître de Conférences à la Faculté de droit de l'UNamur, Post-doctorante dans le cadre de la Chaire e-Gouvernement de l'UNamur[1]

RÉSUMÉ

Aujourd'hui, l'administration est engagée dans l'ère de l'*electronic government* ou « e- gouvernement », que l'on appelle aussi « administration électronique ». Ce terme générique désigne l'ensemble des utilisations des technologies de l'information et de la communication dans l'administration, ainsi que les mutations que ces utilisations y engendrent [2].

Ces nouveaux outils technologiques sont utilisés à des fins diverses : alléger les démarches administratives des citoyens, augmenter l'efficacité de la lutte contre la fraude fiscale, automatiser l'octroi de certaines allocations, etc. Pour ce faire, ces outils traitent les nombreuses données personnelles des citoyens qui sont aujourd'hui enregistrées dans les bases de données de l'administration. Ces technologies constituent dès lors une menace de plus en plus inquiétante pour la protection de la vie privée de chaque individu.

Cette problématique fait l'objet d'une thèse de doctorat, récemment défendue à la Faculté de droit de l'Université de Namur et qui sera publiée prochainement [3]. Cette thèse démontre qu'il est possible d'organiser un e-gouvernement à la fois efficace et respectueux du droit fondamental à la protection de la vie privée des citoyens. Cela suppose une modification en profondeur du droit administratif et la mise en place de solutions nouvelles. La présente contribution livre les traits saillants de cette recherche.

---

1 La Chaire e-Gouvernement a été créée en septembre 2013 à l'Université de Namur. Elle a vocation à offrir principalement au secteur public une expertise indépendante en droit et en informatique pour les questions liées à l'e-gouvernement, au travers de missions de consultance, de formation et de recherche scientifique.

2 E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* Thèse défendue à l'Université de Namur en mai 2013, p. 13. Voy. égal. les éléments les plus pertinents mentionnés dans différentes descriptions de l'e-gouvernement reprises dans les documents suivants : Commission des Communautés européennes, « Le rôle de l'administration en ligne (eGovernment) pour l'avenir de l'Europe », COM(2003) 567 final, du 26 septembre 2003, p. 4 ; Commission des Communautés européennes, « L'information émanant du secteur public : une ressource clef pour l'Europe. Livre vert sur l'information émanant du secteur public dans la société de l'information », COM(1998)585, p. 8 ; Observatoire des Droits de l'Internet, « Facteurs de succès de l'e-gouvernement. Avis n°2 », décembre 2003, disponible sur le site http://www.internet-observatory.be ; Banque mondiale, « Definition of E-Government », http://web.worldbank.org ; R. Silcock, « What is e-government ? », *Parliamentary Affairs,* 2001, vol. 54, p. 88 ; D. De Roy, C. de Terwangne et Y. Poullet, « La Convention européenne des droits de l'homme en filigrane de l'administration électronique », *C.D.P.K.,* 2007, p. 310 ; E. Boudry, F. De Rynck, S. Janssens et S. Rotthier, *E-government : nieuwe kans of nieuw probleem,* Bruges, die Keure, 2009, pp. 1 et 2 ; G. Chatillon, « Fondements, principes et nature du droit de l'administration électronique », *in Droit de l'administration électronique. De nouveaux droits pour les usagers. Des nouvelles règles pour les agents* (G. Chatillon dir.), Bruxelles, Bruylant, 2011, pp. 28 et 29 ; P. Trudel, « Existe-t-il un droit public de la gouvernance en ligne ? », *in ibid..,* p. 312 ; F. Bundshuch-Rieseneder, « Governance and e- governance in the frame of Bologna Process », *in Bologna Process, European Construction, European Neighbourhood Policy* (T. Come et G. Rouet dir.), Bruxelles, Bruylant, 2011, p. 260.

3 E. Degrave, *E-gouvernement et protection de la vie privée,* Bruxelles, Larcier, coll. Crids, à paraître en janvier 2014.

SAMENVATTING

Voor de administratie is het tijdperk ingeluid van de *electronic government* of 'e-government', ook 'elektronische administratie' genoemd. Deze generieke term verwijst naar het geheel van toepassingen van informatie- en communicatietechnologieën in de administratie, evenals de omwentelingen die ze er teweegbrengen. [4]

Deze nieuwe technologische instrumenten worden voor allerlei doeleinden gebruikt: minder administratieve rompslomp voor de burgers, een doeltreffender aanpak van fiscale fraude, automatische toekenning van bepaalde uitkeringen, enz. Daarvoor worden talrijke persoonsgegevens van de burgers verwerkt, die in de gegevensbanken van de administratie geregistreerd zijn. Die technologie vormt dan ook een almaar grotere bedreiging voor de bescherming van de persoonlijke levenssfeer van de burgers.

Deze problematiek werd onder de loep genomen in een doctoraatsthesis, die recent werd verdedigd aan de Faculteit Rechten van de Universiteit van Namen en die binnenkort wordt gepubliceerd. [5] De thesis toont aan dat e-government die tegelijk doeltreffend is en het fundamentele recht op de bescherming van de levenssfeer van de burgers naleeft, wel degelijk mogelijk is. Maar dat vereist een grondige wijziging van het administratief recht en de implementatie van nieuwe oplossingen. Dit artikel behandelt de belangrijkste punten van die zoektocht.

I. L'état des lieux

L'administration est profondément transformée par la technologie, tant dans sa structure que dans son fonctionnement. Jusqu'à présent, l'administration était organisée en « silos ». Dans ce modèle, chaque institution fonctionne de manière autonome, séparée des autres. Elle collecte auprès des citoyens les informations dont elle a besoin pour accomplir ses propres missions. Elle a ses propres fichiers, ses propres outils d'analyse.

Aujourd'hui, on est entré dans l'ère de l'e-gouvernement. Progressivement, on s'oriente vers une administration « en réseaux ». Dans pareille structure, les administrations qui ont un objet de travail commun sont regroupées au sein d'un ensemble qualifié de « réseau sectoriel », comprenant en son cœur une « Banque-carrefour ». Ensuite, chaque administration est chargée d'enregistrer certaines données et d'en assurer la fiabilité et la mise à jour. Lorsqu'une administration a besoin d'une information dont elle ne dispose pas, elle la demande à la Banque-carrefour. Cette dernière est alors chargée d'aller chercher l'information là où elle se trouve et de l'acheminer vers l'administration qui l'a demandée.

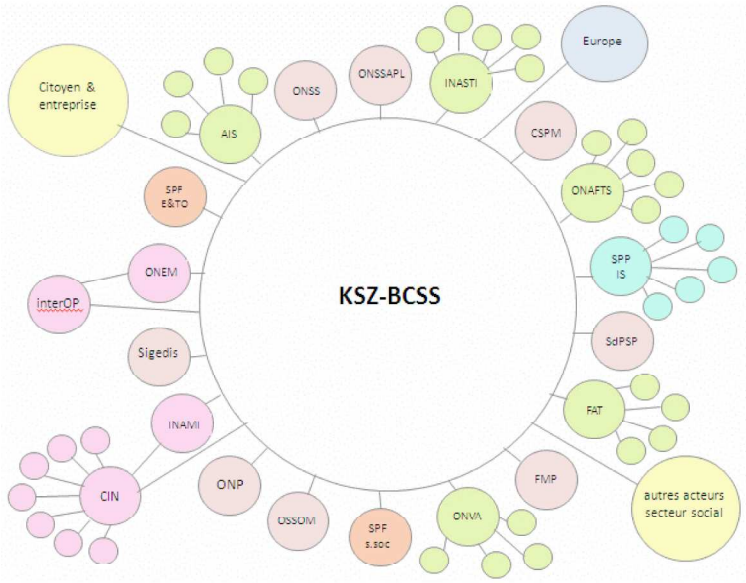
Le réseau de la sécurité sociale, qui comprend en son cœur la Banque-carrefour de la sécurité sociale, est un exemple emblématique de cette structure administrative nouvelle. Schématiquement, elle se présente comme suit[6] :

---

[4] E. Degrave, *L'e-gouvernement et la protection de la vie privée. Légalité, transparence et contrôle,* doctoraatsthesis verdedigd aan de Universiteit van Namen in mei 2013, p. 13. Zie ook de meest relevante elementen vermeld in verschillende beschrijvingen van e-gouvernement in de volgende documenten: Commissie van de Europese Gemeenschappen, 'The role of e-Government for Europe's future', COM(2003) 567 final, van 26 september 2003, p. 4; Commissie van de Europese Gemeenschappen, 'Public Sector Information : a Key Resource for Europe. Green Paper on Public Sector Information in the Information Society', COM(1998)585, p. 8; Observatorium van de Rechten op het Internet, 'Succesfactoren van het e-government, Advies nr. 2', december 2003, beschikbaar op de website http://www.internet-observatory.be; Wereldbank, 'Definition of E-Government', http://web.worldbank.org; R. Silcock, 'What is e-government?', *Parliamentary Affairs,* 2001, vol. 54, p. 88; D. De Roy, C. de Terwangne en Y. Poullet, 'La Convention européenne des droits de l'homme en filigrane de l'administration électronique', *C.D.P.K.,* 2007, p. 310; E. Boudry, F. De Rynck, S. Janssens en S. Rotthier, *E- government: nieuwe kans of nieuw probleem,* Bruges, die Keure, 2009, p. 1 en 2; G. Chatillon, 'Fondements, principes et nature du droit de l'administration électronique', *in Droit de l'administration électronique. De nouveaux droits pour les usagers. Des nouvelles règles pour les agents* (G. Chatillon dir.), Brussel, Bruylant, 2011, p. 28 en 29; P. Trudel, 'Existe-t-il un droit public de la gouvernance en ligne?', *in ibid.,* p. 312; F. Bundshuch-Rieseneder, 'Governance and e-governance in the frame of Bologna Process', *in Bologna Process, European Construction, European Neighbourhood Policy* (T. Come en G. Rouet dir.), Brussel, Bruylant, 2011, p. 260.

[5] E. Degrave, *E-gouvernement et protection de la vie privée,* Brussel, Larcier, coll. Crids, te verschijnen in januari 2014.

[6] Ce schéma est disponible sur le site de la Banque-Carrefour de la sécurité sociale, à l'adresse www.ksz- bcss.fgov.be/fr/bcss/page/content/websites/belgium/about/mission/structure.html



Ce système présente des avantages pour le citoyen qui voit ses démarches administratives considérablement allégées. Par exemple, un demandeur d'emploi qui désire obtenir l'allocation de chômage s'adresse à l'ONEM. Pour calculer le montant de l'allocation de chômage, l'ONEM doit disposer de certaines informations telles que le montant des allocations familiales perçues par le demandeur d'emploi. Jadis, le demandeur d'emploi devait fournir lui-même à l'ONEM le document pertinent pour établir cette information, à défaut de quoi, le paiement de l'allocation de chômage lui était refusé. Aujourd'hui, en vertu de l'article 11 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, l'ONEM ne peut obtenir cette information qu'en la demandant à la Banque-carrefour de la sécurité sociale, et non plus à la personne concernée. En effet, les données relatives aux allocations familiales payées aux citoyens sont enregistrées dans la base de données de l'ONAFTS, institution qui se trouve dans le réseau de la sécurité sociale tout comme l'ONEM. Un demandeur d'emploi ne peut donc plus se voir refuser l'allocation de chômage au motif qu'il n'a pas fourni une information qui se trouve dans le réseau de la sécurité sociale.

Ce système contribue également à l'efficacité de l'administration, puisqu'il permet notamment un échange rapide d'informations en principe exactes et à jour. En outre, puisque ces données sont disponibles sous forme informatisée dans les administrations, on peut les réutiliser et y appliquer différents traitements. C'est ce que l'on fait notamment pour contrôler plus efficacement les citoyens. Par exemple, progressivement, se mettent en place des outils de profilage pour lutter contre la fraude fiscale et sociale. Il s'agit de regrouper des données très différentes au sein d'une grande base de données appelée « entrepôt de données » ou « *datawarehouse* » et d'y appliquer des calculs très puissants appelés « algorithmes de fraude », basés notamment sur des calculs statistiques. Ce faisant, l'ordinateur peut identifier des personnes suspectées de fraude. Ces outils sont très efficaces puisqu'en général, la personne suspectée de fraude se révèle, après contrôle, être effectivement coupable de fraude. Prenons un exemple simplifié à l'extrême pour la clarté du propos : Elise Degrave est assistante à l'université. Elle est donc réputée avoir un maigre salaire. Or, elle déclare à la DIV qu'elle roule en Porsche, elle déclare au Cadastre qu'elle habite à Lasne et elle déclare à l'Urbanisme qu'elle fait construire une piscine. Le croisement de ces données aboutira certainement à conclure que la situation fiscale d'Elise Degrave est suspecte. Un contrôle fiscal sera encouragé.

De toute évidence, l'e-gouvernement est donc séduisant. Mais il est aussi dangereux. En général, lorsqu'on évoque le danger d'utiliser les technologies dans l'administration, on songe au spectre de *Big Brother.* C'est l'idée d'un Etat omniscient, qui saurait tout de tout le monde et pourrait surveiller chaque individu. Cette crainte est justifiée. Mais il existe également un autre danger tout aussi fondamental, plus rarement mis en évidence : celui de créer progressivement une administra-

tion kafkaïenne[7], c'est-à-dire, une administration à ce point technique et complexe, à ce point distante, qu'elle en deviendrait incompréhensible et dès lors, incontrôlable.

Face à ce constat, la question qui anime la recherche est la suivante : comment faire en sorte que, dans l'e-gouvernement, le citoyen ne soit pas exclu de cette évolution technologique et qu'il puisse continuer à comprendre et contrôler l'action de l'administration ? La réponse à cette question en appelle au droit à la protection de la vie privée et au droit administratif.

II. L'e-gouvernement aux confins du droit à la protection de la vie privée et du droit administratif

La thèse démontre qu'il est possible d'organiser un e-gouvernement efficace tout en octroyant au citoyen les moyens nécessaires pour garder une prise sur l'administration, afin de la comprendre et de la contrôler. De cette manière, l'efficacité de l'administration est encouragée, et le droit à la vie privée des individus est protégé.

Pour atteindre ce double objectif, il s'impose de créer un cadre juridique pour l'e-gouvernement, qui soit cohérent et adapté aux dangers de l'informatisation de l'administration.

Actuellement, l'e-gouvernement est soumis à un double régime juridique.

D'une part, le régime juridique de la protection de la vie privée et des données à caractère personnel[8] doit être respecté, puisque le fonctionnement de l'e-gouvernement est fondé en grande partie sur le traitement informatisé des données personnelles des citoyens. Le droit à la vie privée s'entend aujourd'hui du droit à l'autodétermination informationnelle[9]. Concrètement, cela signifie que chacun a le droit d'être conscient du fait que ses données circulent et sont traitées, de vérifier qu'elles sont exactes, de contester les abus dans l'utilisation des données et d'obtenir réparation du dommage éventuellement subi suite à ces abus. Il y a donc lieu de mettre en place les moyens nécessaires pour garantir au citoyen la satisfaction de telles prérogatives dans l'e-gouvernement.

D'autre part, bien que l'administration se modernise considérablement, les règles de droit administratif général restent d'application. Or, ces vieilles règles, applicables depuis toujours à l'administration, ont été pensées en dehors de toute préoccupation liée aux technologies. Elles doivent aujourd'hui recevoir une interprétation nouvelle, adaptée aux enjeux de l'e-gouvernement.

Ainsi, pour organiser un cadre juridique cohérent pour l'e-gouvernement, il s'impose de réfléchir à l'articulation entre le régime juridique de la protection de la vie privée et des données à caractère personnel et le droit administratif. Ce n'est pas une tâche aisée puisque ces deux corps de règles sont fort distincts. De plus, de manière générale, la littérature scientifique consacrée à l'e-gouvernement est maigre. Les administrativistes délaissent bien souvent les questions de droit administratif soulevées par les technologies, comme s'ils craignaient les ordinateurs. Le même constat vaut pour les spécialistes de la protection des données, qui semblent peu à l'aise dans les méandres du droit administratif.

La thèse montre que ces deux mondes peuvent dialoguer et apporter une réponse aux questions soulevées par l'e-gouvernement. Il est, en effet, possible de greffer les règles de protection des données sur les règles de droit administratif. On voit apparaître une cohérence dans les règles actuellement applicables à l'e-gouvernement. Mais il faut aussi aller plus loin pour répondre aux dangers de l'e-gouvernement, en dégageant des solutions nouvelles.

III. La légalité, la transparence et le contrôle de l'e-gouvernement

La démonstration effectuée dans la thèse est structurée au départ de trois piliers de l'Etat de droit que sont la

---

7 D. Solove, " 'I've got nothing to hide' and other misunderstandings of privacy", *San Diego Law Review,* 2007, vol. 44, 745, 2007, pp. 745 à 772.

8 Ce régime juridique est formé de l'article 8 de la Convention européenne des droits de l'homme, de l'article 22 de la Constitution, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, et de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

9 Voy. not. Y. Poullet et A. Rouvroy, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel. Une réévaluation de l'importance de la vie privée pour la démocratie », *in Etat de droit et virtualité* (K. Benyekhlef et P. Trudel dir.), Montréal, Thémis, 2009, pp. 169 et s.

légalité, la transparence et le contrôle de l'administration. Ces trois exigences fondamentales sont particulièrement ébranlées par l'e-gouvernement tel qu'il se développe actuellement. Partant de ce constat, la recherche dégage des solutions pour assurer le respect de ces exigences dans le contexte de l'e- gouvernement.

A. La légalité de l'e-gouvernement

Comment le législateur doit-il encadrer l'e-gouvernement ?

Les outils de traitement de données sont des ingérences dans la vie privée des citoyens. En vertu de l'exigence de légalité imposée par l'article 8 de la Convention européenne des droits de l'homme et l'article 22 de la Constitution, ces outils doivent être encadrés par une loi [10]. Deux raisons justifient l'intervention du législateur. D'une part, l'exigence de légalité doit conduire à soumettre au débat démocratique l'organisation d'ingérences dans la vie privée des citoyens [11]. En particulier, il importe de veiller à ce que les traitements de données à caractère personnel effectués dans l'administration incarnent un juste équilibre entre l'efficacité administrative et la protection de la vie privée des citoyens. Ce travail doit être effectué par le législateur. Si l'organisation de traitements de données était laissée exclusivement à la discrétion des administrations, celles-ci pourraient avoir tendance à apprécier la nécessité de tels traitements principalement au regard de leur intérêt immédiat, celui de l'efficacité administrative, et de donner trop peu de poids à la protection de la vie privée des citoyens. D'autre part, la loi doit être accessible et prévisible. De cette manière, les citoyens peuvent prendre connaissance des ingérences organisées dans leur vie privée. L'accessibilité et la lisibilité des textes organisant des ingérences dans la vie privée importent particulièrement lorsqu'il est question de traitements de données à caractère personnel. En effet, l'utilisation d'informations personnelles fait peur aux citoyens car les outils nouveaux de traitements de données paraissent complexes et opaques. Les personnes concernées craignent également que l'objectif poursuivi lors de la collecte de leurs informations soit détourné et se retourne finalement contre eux. L'exigence de prévisibilité de la norme prend dès lors tout son sens pour établir la confiance entre les citoyens et l'Etat qui met en place de tels outils.

Malheureusement, pour l'heure, on constate que des aspects importants de l'e-gouvernement ne sont pas organisés par le législateur. Par ailleurs, lorsqu'elles existent, les lois qui encadrent l'e-gouvernement ne répondent pas pleinement à cette exigence de légalité. En effet, l'e-gouvernement est soumis à des normes multiples, éparses et, dès lors, difficilement accessibles. Celles-ci sont également peu compréhensibles, tant le jargon lié à l'e-gouvernement est technique et complexe. Enfin, certaines lois prennent la forme de loi « fourre-tout », ou de « loi-programme », si bien que les traitements de données ainsi organisés n'ont pas fait l'objet d'un réel débat démocratique.

Face à ce constat, comment le législateur doit-il encadrer l'e-gouvernement pour répondre, d'une part, à l'exigence constitutionnelle de légalité, tout en tenant compte, d'autre part, des contraintes de l'e- gouvernement qui s'opposent à une interprétation trop stricte de cette exigence constitutionnelle ? Plus précisément, à quels critères le législateur peut-il se référer pour encadrer au mieux les traitements de données dans l'administration ?

L'analyse des arrêts de la Cour constitutionnelle et des avis de la section de législation du Conseil d'Etat rendus en la matière révèle que le législateur doit définir lui-même les éléments essentiels d'un traitement de données à caractère personnel. Il s'agit, par exemple, du type de données enregistrées dans une base de données, des institutions qui peuvent accéder à ces informations, de la durée d'enregistrement de ces données, etc. Le rôle du législateur est donc ample. Cela a des consé-

---

[10] J. Vande Lanotte et G. Goedertier, *Handboek Belgisch Publiekrecht*, Bruges, die Keure, 2010, pp. 448- 449, n° 688 ; P. De Hert, « Artikel 8. Recht op privacy », *in Handboek EVRM, Deel 2. Artikelsgewijze commentaar* (J. Vande Lanotte et Y. Haeck dir.), Anvers, Intersentia, 2004, pp. 716-718 ; M. Melchior et C. Courtoy, *op. cit.,* p. 284 ; R. Andersen et C. Behrendt, « La protection des droits constitutionnels », *in Les droits fondamentaux en Belgique* (M. Verdussen et N. Bonbled dir.), *op. cit.,* p. 356; E. Degrave, « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.,* 2009, p. pp. 368 - 370.

[11] Le Cour constitutionnelle et la section de législation du Conseil d'Etat l'ont rappelé à plusieurs reprises. Voy. Avis L. 37.765/1/2/3/4 du 4 novembre 2004 sur un avant-projet de loi-programme, *Doc. Parl.,* Chambre, 2004-2005, n° 1437 ; avis L. 37.748 et 37.749/AG du 23 novembre 2004 sur un avant-projet de loi modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (37.748/AG) et sur un avant-projet de loi modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitation de sécurité (37.749/AG), *Doc. Parl*., Chambre, 2004-2005, n° 1598/1 et 1599/1, cités par P. Nihoul, M. Joassart et V. Franck, « Le Conseil d'Etat. Chronique de jurisprudence – 2004 », *R.B.D.C.*, 2005/2, p. 260, n° 6 ; C.C., arrêt n° 202/2004, du 21 décembre 2004, B.4.3. et B.6.3. ; C.C., arrêt n° 95/2008, du 26 juin 2008, B.42 ; C.C., arrêt n° 29/2010, du 18 mars 2010, B. 16.1 ; C.C., arrêt n° 6/2013, du 14 février 2013, B.5.7 ; C.C., arrêt n° 66/2013, du 16 mai 2013, B.11.1.

quences sur le rôle du Roi qui, sans être réduit à néant, est néanmoins fortement diminué dans l'e-gouvernement.

Il n'en demeure pas moins que, malgré la mise en lumière des éléments essentiels du traitement, la tâche du législateur demeure assez floue. Par exemple, comment déterminer les données qui doivent figurer dans une base de données ? Comment choisir entre un numéro d'identification unique ou un numéro d'identification sectoriel ? A quelles conditions peut-on mettre en place un « *datawarehouse* » pour lutter contre la fraude fiscale et sociale ? Le législateur doit être guidé dans de tels choix. Le régime juridique de la protection des données à caractère personnel l'y aide, en organisant une exigence de finalité et une exigence de proportionnalité

La thèse montre que le régime juridique de la protection des données à caractère personnel, s'il est correctement appliqué, offre au législateur des critères qui lui permettent de mieux légiférer. Ainsi, d'une part, le traitement de données doit poursuivre une finalité précise, compatible et légitime. D'autre part, le critère de proportionnalité impose un examen minutieux du caractère nécessaire et approprié du traitement mis en place et des données utilisées. Malheureusement, ces critères sont assez flous et posent de nombreuses questions en pratique. Il en va d'autant plus ainsi que peu de doctrine et peu de jurisprudence aident à comprendre la manière de les appliquer dans le secteur public. La thèse propose donc des interprétations de ces critères, fondées notamment sur les avis de la Commission de la protection de la vie privée, étudiés depuis 1992 jusqu'à 2013.

Enfin, la thèse encourage le législateur à poser un choix politique clair et cohérent. Il faut dépasser l'« entre-deux » qui caractérise l'administration actuelle, située entre le modèle de l'administration en silos et le modèle de l'administration en réseaux. On encourage le législateur à s'engager franchement dans le modèle de l'administration en réseaux, tout en veillant au respect des règles de protection de la vie privée. Par ailleurs, des solutions nouvelles doivent être mises en place, notamment en adoptant une loi-cadre propre à l'e-gouvernement.

B. La transparence de l'e-gouvernement

Comment savoir ce que l'administration détient sur chaque individu et où se trouvent ces données dans l'administration ?

La réponse à cette question intéresse notamment celui qui souhaite vérifier l'exactitude des données enregistrées à son sujet. Cette curiosité légitime est particulièrement importante dans la structure administrative nouvelle. En effet, puisque celle-ci est fondée sur la réutilisation maximale des données des citoyens, les éventuelles erreurs qui affectent ces informations risquent d'être reproduites à de multiples reprises.

Le droit administratif consacre des règles de transparence administrative. En principe, celles-ci permettent aux citoyens d'accéder aux documents administratifs. Dans le contexte de l'e-gouvernement, ces règles sont intéressantes pour obtenir, par exemple, des documents qui expliquent la structure et le fonctionnement l'administration informatisée.

Le régime juridique de la protection des données à caractère personnel organise des moyens de transparence complémentaires, qui permettent au citoyen d'accéder à ses données à caractère personnel. Chaque personne peut ainsi savoir ce que l'administration détient sur elle, dans quel but, à qui ces données ont été ou seront transmises, etc.

Les voies d'accès organisées par le droit administratif et par le droit de la protection des données à caractère personnel ont fait l'objet d'une démarche empirique menée durant la thèse. Il s'est agi de tester concrètement les droits offerts au citoyen en matière de transparence des documents administratifs et des données à caractère personnel, en les exerçant auprès de différentes administrations. De cette manière, des obstacles concrets à la transparence de l'e-gouvernement ont pu être identifiés. Ils tiennent principalement au fait que les règles actuelles de transparence ont été conçues par rapport à une administration fonctionnant avec du papier (et non des technologies informatiques) et structurée en silos (et non en réseaux). Il en résulte que la publicité de l'administration est aujourd'hui davantage passive qu'active, reposant essentiellement sur les démarches des citoyens et non sur les initiatives de l'administration. Les procédures à suivre pour exercer les droits d'accès sont lourdes et difficilement compréhensibles, ce qui soulève maintes difficultés dans l'e-gouvernement.

Partant de ces constats, la thèse dégage des solutions, en encourageant notamment le basculement de la publicité passive de l'administration vers une publicité active de celle-ci qui soit beaucoup plus généralisée et effective, de manière à organiser une réelle transparence de l'e-gouvernement.

Aujourd'hui, le développement de la publicité active de l'administration est rendu possible par les technologies existantes. Pareil développement est également néces-

saire à l'ère de l'e-gouvernement. En effet, pour éviter le danger de créer une administration kafkaïenne qui échapperait au contrôle des citoyens, il importe de permettre à ces derniers d'exercer une prise sur les institutions publiques. C'est pourquoi, un équilibre raisonnable doit être organisé entre les pouvoirs de l'administration et ceux du citoyen. Cela suppose que les technologies utilisées par l'administration pour augmenter son efficacité bénéficient également au citoyen désireux de prendre connaissance du sort réservé à ses données dans l'administration. Comme l'exprime un auteur, quand l'administration roule en limousine, on ne peut pas imposer aux citoyens d'avancer à pied[12]**...**

Ainsi suggère-t-on notamment la mise en place d'un portail internet dédié à la transparence. Après s'être identifié à l'aide de sa carte d'identité électronique, chaque citoyen devrait pouvoir accéder à un panorama de la localisation de ses données dans l'administration. En cliquant sur les bases de données mentionnées, il pourrait visualiser les données enregistrées à son sujet, vérifier leur exactitude et signaler les éventuelles erreurs affectant ces informations. Il devrait également pouvoir obtenir un traçage du chemin parcouru par les données dans l'administration, grâce au mécanisme de l'*audit trail,* qui, le cas échéant, ferait apparaître les utilisations illégales desdites données. Ainsi, les abus dans l'utilisation des données pourraient faire l'objet d'un recours à la Commission de la protection de la vie privée et/ou devant les cours et tribunaux.

C. Le contrôle de l'e-gouvernement

Comment garantir au citoyen que l'administration respecte le droit et est sanctionnée si tel n'est pas le cas ?

Le droit public organise des recours qui, s'ils sont exercés, sont efficaces. Ainsi, entre autres exemples, une loi qui organise un traitement de données à caractère personnel peut être annulée par la Cour constitutionnelle si elle porte atteinte au droit fondamental à la protection de la vie privée, consacré par l'article 22 de la Constitution. Une décision administrative peut être annulée par le Conseil d'Etat, section du contentieux administratif, s'il est établi qu'elle a été adoptée à partir de données que l'auteur de l'acte n'avait pas le droit d'utiliser. C'est le cas, par exemple, si le transfert de données n'a pas été autorisé par un comité sectoriel alors qu'il aurait dû l'être.

Le Tribunal du Travail peut mettre à néant la décision du CPAS qui refuserait le versement du revenu d'intégration sociale au motif que le demandeur n'aurait pas fourni certaines informations s'il est établi que le CPAS avait l'obligation de trouver ces informations par lui-même, via la Banque-carrefour de la sécurité sociale[13]**.**

Malheureusement, ces recours souffrent de deux défauts majeurs. D'une part, en général, les citoyens ne les exercent pas. Bien souvent, ils n'ont pas connaissance des illégalités commises dans l'administration. Mais, au-delà, quand bien même ils les connaîtraient, il y a fort à parier qu'ils ne consacreraient pas du temps et de l'argent à contester ces problèmes qui les dépassent largement. D'autre part, quand ces illégalités sont effectivement attaquées, on constate que les avocats n'invoquent pas ou invoquent mal les règles de protection des données. Certains arrêts laissent ainsi apparaître que des arguments tirés de la protection des données n'ont pas été invoqués alors qu'ils auraient pu être porteurs.

Le régime juridique de la protection des données organise d'autres moyens d'action, davantage adaptés à l'univers technologique. En particulier, la Commission de la protection de la vie privée joue un rôle essentiel. Elle dispose de moyens d'action intéressants dans le contexte de l'e-gouvernement. A l'image du Médiateur fédéral, la Commission de la protection de la vie privée reçoit les plaintes des citoyens lorsqu'elles touchent à la protection de la vie privée. Une médiation peut ensuite être organisée entre la personne concernée et l'institution visée. D'autres moyens d'action sont à sa disposition, tels que le droit d'intenter une action judiciaire dans l'intérêt collectif [14]. Les traitements de données illégaux commis dans l'administration peuvent ainsi être dénoncés en justice par l'autorité de protection des données.

Néanmoins, à certains égards, le contrôle exercé par la Commission de la protection de la vie privée manque, lui aussi, d'efficacité et d'effectivité. Par exemple, cette institution n'a encore jamais exercé l'action judiciaire dans l'intérêt collectif. Ce recours reste d'ailleurs assez méconnu. Par ailleurs, le statut de la Commission de la protection de la vie privée soulève de multiples interrogations. Entre autres questions, cette institution est-elle une autorité administrative ? Dans la négative, ses décisions ne seraient pas attaquables devant le Conseil d'Etat, section du contentieux administratif, ce qui pose maintes

---

[12] D.W. Schartum, « Access to Governement-Held Information : Challenges and Possibilities », *The Journal of Information Law and Technology,* 1998/1, § 7.1. (traduction libre).

[13] Pour un cas de jurisprudence, voy. not. C. trav. Bruxelles (8è ch.), 21 avril 2010, R.G. n° 2008/AB/51591 et n° 2009/AB/51809.

[14] Voy. l'article 32 de la loi du 8 décembre 1992 sur la protection de la vie privée à l'égard des traitements de données à caractère personnel.

difficultés dans un Etat de droit. En outre, certaines dispositions du régime juridique européen de protection des données imposent que l'autorité nationale de protection des données soit indépendante. La Cour de justice de l'Union européenne donne une portée très large à cette exigence, comme en témoignent deux arrêts rendus récemment [15]. La Commission de la protection de la vie privée est-elle suffisamment indépendante au regard du prescrit européen ? Cette question en appelle une autre : comment concilier l'exigence européenne d'indépendance avec notre système constitutionnel, qui s'oppose à ce qu'une autorité dotée d'un pouvoir de décision échappe au contrôle de tutelle ? La Cour constitutionnelle a été amenée à se pencher sur cette question. L'arrêt rendu est étonnant.

La thèse entend résoudre ces questions au regard du droit constitutionnel, du droit administratif et du droit de la protection des données. S'agissant de l'efficacité de la Commission de la protection des données, par exemple, le législateur est encouragé notamment à conférer plus de moyens d'action à notre autorité de protection des données, tels qu'un pouvoir d'admonestation et un pouvoir d'amende, comme en dispose déjà son homologue français, la Commission Nationale Informatique et Libertés (« CNIL »). Pour clarifier le statut de la Commission de la protection des données, on identifie notamment des solutions jurisprudentielles et législatives qui permettraient de qualifier cette institution d'autorité administrative. Des pistes sont également proposées pour résoudre la tension entre le droit européen et le droit constitutionnel belge que créent les exigences d'indépendance et de contrôle imposées à la Commission de la protection de la vie privée.

Conclusion

Le développement de l'e-gouvernement provoque de profonds bouleversements dans le fonctionnement et la structure de l'administration. Nombre d'outils et de traitements informatiques nouveaux augmentent désormais l'efficacité de l'action administrative. Cela génère beaucoup d'enthousiasme. Néanmoins, des craintes surgissent également, en particulier s'agissant de la protection de la vie privée des citoyens dont les nombreuses données personnelles sont enregistrées et utilisées par les institutions publiques. Comment endiguer le danger d'un *Big brother* et d'une administration kafkaïenne ?

La thèse, expliquée succinctement dans le présent article, entend démontrer qu'il est possible d'organiser un e-gouvernement efficace tout en protégeant la vie privée des citoyens. Pour ce faire, il importe de donner à ces derniers des moyens pour garder une prise sur l'administration, afin de la comprendre et de la contrôler. Cela suppose de confronter l'e-gouvernement au régime juridique de la protection de la vie privée et des données à caractère personnel, d'une part, et au droit administratif général, d'autre part. On constate alors que le droit administratif doit être modernisé et enrichi à la lumière des préoccupations de protection des données. De cette manière, on peut espérer rééquilibrer la relation entre le citoyen et l'administration, aujourd'hui menacée dans l'e-gouvernement. La démonstration est effectuée au départ de trois piliers de l'Etat de droit que sont la légalité, la transparence et le contrôle de l'administration.

Finalement, l'e-gouvernement donne au droit administratif une dimension nouvelle qui semble désormais fondé sur trois axes. Le premier axe existe depuis toujours : le droit administratif organise les services de l'administration. Le deuxième axe est apparu au début des années nonante, avec l'adoption des règles relatives à la transparence de l'administration : l'administration doit s'ouvrir au citoyen, pour établir un dialogue avec lui. Le troisième axe apparaît avec l'e-gouvernement : l'administration doit non seulement s'ouvrir au citoyen mais il doit également devenir un outil de protection du citoyen contre l'administration qui commettrait des abus dans l'utilisation de ses données à caractère personnel.

En définitive, au-delà de son apparente technicité, l'e-gouvernement apparaît aujourd'hui comme une chance offerte au droit administratif de rapprocher l'administration et les citoyens, en se nourrissant d'un idéal humain fort qui désormais l'irrigue, celui de protéger la vie privée des individus et de contribuer ainsi à créer les conditions de leur libre épanouissement personnel.

***

[15] C.J.U.E., gde ch., 9 novembre 2010, *République fédérale d'Allemagne c. Commission*, C-518/07; C.J.U.E., gde ch., 16 octobre 2012, *République d'Autriche c. Commission,* C-614/10.