

« Facteurs de succès de l'e-gouvernement »

Avis n° 2 de l'Observatoire des Droits de l'Internet

Observatoire des Droits de l'Internet

« L'Internet en toute confiance »



<http://www.internet-observatory.be>

Notes de l'éditeur

Site internet

<http://www.internet-observatory.be>

Remerciements

L'avis est imprimé par le [Service public fédéral Economie, P.M.E., Classes moyennes et Energie](#). L'Observatoire des Droits de l'Internet remercie le personnel qui a contribué à l'impression de cet avis.

Commande

L'avis peut être téléchargé (en format pdf) sur le site internet de l'Observatoire des Droits de l'Internet :

http://www.internet-observatory.be/internet_observatory/pdf/advice/fr_002.pdf

L'avis peut aussi être obtenu par courrier, dans la mesure des stocks disponibles. Dans ce cas, veuillez envoyer votre demande au [secrétariat](#) de l'Observatoire des Droits de l'Internet en mentionnant le titre de l'avis et votre adresse.

*Observatoire des Droits de l'Internet
Secrétariat
Rue de l'Industrie 6
1000 Bruxelles*

Copyright

Aucune forme de cette publication ne peut être reproduite et/ou publiée au moyen d'impression, photocopie, microfilm, ou autre moyen quelconque sans autorisation préalable de l'éditeur.

Editeur responsable

Thibault VERBIEST, Rue de l'Industrie 6, 1000 Bruxelles

Dépôt légal

D2003/1226/33

Date de publication

Décembre 2003

Table des matières

NOTES DE L'ÉDITEUR.....	2
TABLE DES MATIÈRES.....	3
RÉSUMÉ	5
1. QU'EST-CE QUE L'E-GOUVERNEMENT ?	7
2. L'APPROCHE BELGE	7
3. CONDITIONS-CADRES	9
4. ANNEXE	14

Le présent avis porte sur l'e-gouvernement. Il a été approuvé à l'unanimité des membres présents lors de la séance plénière de [l'Observatoire des Droits de l'Internet](#) qui s'est tenue à Bruxelles le 3 décembre 2003.

Résumé

Dans cet avis, l'Observatoire des Droits de l'Internet (ci-dessous l'Observatoire) indique tout d'abord que le gouvernement électronique (e-gouvernement) doit aller de pair avec la simplification administrative. Dès lors, il convient avant tout d'optimiser les procédures dans le back office des pouvoirs publics et d'avoir recours à l'échange de données nécessaires entre les différents services publics, dans le respect de la législation sur les données à caractère personnel. Ensuite, les efforts de communication consentis jusqu'à présent sont très limités. Les entreprises et les citoyens ne sont donc pas suffisamment informés sur les services en ligne déjà disponibles et sur ce qui se prépare. Il paraît indispensable que les pouvoirs publics consacrent à court terme suffisamment de moyens et les ressources humaines nécessaires à leur plan d'action. Enfin, des conditions cadres ont été formulées dans trois domaines, notamment en ce qui concerne l'accessibilité des services de l'e-gouvernement, la connaissance des attentes des citoyens et des entreprises, et enfin le renforcement de leur confiance dans l'e-gouvernement.

1. Qu'est-ce que l'e-gouvernement ?

Le gouvernement électronique (e-gouvernement) consiste à développer la prestation de services par les pouvoirs publics en utilisant au maximum les possibilités offertes par les nouvelles technologies de l'information et de la communication (TIC). Cela implique de repenser en profondeur l'interaction entre les pouvoirs publics eux-mêmes et, d'une part, entre les pouvoirs publics et les entreprises, d'autre part, entre les pouvoirs publics et les citoyens.

Le fondement du gouvernement électronique est que, grâce à la simplification des procédures, le traitement et la réutilisation accélérés d'informations déjà disponibles aboutissent à la simplification administrative. Par conséquent, on ne peut parler d'e-gouvernement s'il s'agit uniquement d'un projet de *front office* qui n'utilise qu'une application internet, allant de la mise à disposition d'informations, à l'exécution de déclarations électroniques jusqu'au traitement électronique complet d'un dossier qui reprend les procédures existantes. C'est surtout le *back office* (traitement interne aux services publics) qui doit être associé à un projet de gouvernement électronique afin que les procédures soient assouplies, que les services publics échangent des informations entre eux (sous réserve de ce qui sera dit *infra*, point 3.3.2) et que les formalités désormais superflues soient supprimées. A cet égard, il faut souligner que les citoyens et les entreprises qui ne recourent pas aux services de l'e-gouvernement bénéficieront également de cette réorganisation du *back office*.

2. L'approche belge

Il ressort d'une [étude](#) comparative internationale demandée par la [Commission européenne](#)¹ que la Belgique enregistre un retard dans les applications du gouvernement électronique.

Toutefois, notre pays est en train de rattraper considérablement son retard au sein de l'Union européenne. En effet, le faible nombre de projets visibles en la matière ne signifie pas qu'il ne s'y passe rien. Une des raisons du retard relatif dans la disponibilité des services en ligne en Belgique est la priorité accordée aux adaptations du *back office* avant la mise à disposition, pour le public, des applications en *front office*, ce qui crée une bonne base pour développer rapidement et efficacement des applications de *front office*.

¹ European Commission DG information Society, "Web-based survey on electronic public services", février 2003.

Un certain nombre de principes sont essentiels dans l'élaboration de l'e-gouvernement en Belgique :

- partir des problèmes ou des questions des citoyens et des entreprises ;
- partager et échanger les données entre les services publics (sous réserve de ce qui sera dit *infra*, point 3.3.2) ;
- créer un portail d'accès commun aux différents services publics (au fédéral mais aussi notamment au fédéral-régional).

Une des conséquences de ces principes est que depuis un certain temps, la (ré)organisation du *back office*, l'élaboration de l'infrastructure technique et la coopération entre projets à différents niveaux des pouvoirs publics manquent de transparence.

Le développement relativement plus lent du gouvernement électronique en Belgique peut se justifier à condition que les efforts susmentionnés aboutissent à des services efficaces. Les entreprises attendent beaucoup de projets structurels tels que la [Banque-Carrefour des Entreprises](#), le [site portail](#) et les [déclarations électroniques de la sécurité sociale](#). Les citoyens pourront non seulement rechercher plus rapidement et plus efficacement les informations nécessaires en ligne, mais aussi utiliser différentes applications en ligne nécessitant une identification, grâce à la carte d'identité électronique et à la signature électronique.

L'engagement politique de réduire d'un quart les obligations administratives dans un délai de quatre ans était probablement un projet trop ambitieux, vu le manque de moyens, de ressources humaines et la complexité de la tâche.

La principale lacune de la politique actuelle d'e-gouvernement est cependant la communication aux utilisateurs (citoyens et entreprises). Les efforts de communication des pouvoirs publics ont été jusqu'à présent très restreints. Les entreprises et les citoyens sont donc insuffisamment informés des services déjà disponibles en ligne, de ce qui se prépare et de la manière dont ils peuvent ou doivent y répondre. Les projets risquent de ne pas répondre adéquatement aux attentes légitimes des utilisateurs si la communication n'est pas améliorée.

3. Conditions-cadres

3.1. Accessibilité des services de l'e-gouvernement

Les services offerts dans le cadre de l'e-gouvernement doivent être accessibles : pour ce faire, l'Observatoire recommande de réduire la fracture numérique et de garantir la neutralité technologique.

3.1.1. Réduire la fracture numérique

L'e-gouvernement ne sera une réussite que si un grand nombre de citoyens et d'entreprises, convaincus par l'initiative², y recourent. Dès lors, il faut veiller à ce que toutes et tous (ou presque) y aient accès, ce qui suppose un matériel suffisant (hardware et software), une bonne connexion à l'internet et des connaissances de base pour utiliser le tout correctement (le cas échéant en organisant des formations). L'Observatoire recommande aussi que, dans la mesure du possible, ces services soient accessibles aux personnes souffrant d'un handicap, visuel notamment.

L'objectif est loin d'être atteint actuellement, même si la situation tend à s'améliorer progressivement. Des recommandations concrètes seront formulées dans un prochain avis de l'Observatoire, consacré à la fracture numérique.

3.1.2. Garantir la neutralité technologique

Les applications e-gouvernement doivent être neutres sur le plan technologique. Dès lors que leurs systèmes informatiques (hardware et software) sont raisonnablement configurés, compte tenu des progrès technologiques et des produits disponibles sur le marché, il est impensable que les citoyens ou les entreprises doivent les adapter pour pouvoir utiliser des applications e-gouvernement. Dans ce cadre, les autorités publiques doivent veiller à l'interopérabilité³ des systèmes pour faire en sorte que les initiatives s'intègrent facilement dans les systèmes informatiques existants : on ne peut, par exemple, priver les citoyens ou les entreprises des services d'e-gouvernement sous prétexte qu'ils ne possèdent pas la dernière version du navigateur ou qu'ils utilisent un système d'exploitation moins répandu.

² Cela requiert une bonne communication et la mise en place de campagnes de promotion et de sensibilisation, notamment (voy. point 2, *in fine*).

³ Par interopérabilité, on vise la capacité qu'ont deux systèmes de se comprendre l'un l'autre et de fonctionner en synergie. L'objectif est que les données fournies par l'administration puissent être exploitées par le citoyen ou l'entreprise.

3.2. Connaître les attentes des citoyens et des entreprises

L'e-gouvernement est avant tout destiné aux entreprises et aux citoyens, qui en sont les principaux bénéficiaires. Il convient donc de s'interroger sur leurs attentes et leurs revendications, et évaluer ce que l'administration électronique est susceptible de leur apporter. Les priorités doivent porter sur des démarches moins nombreuses, plus simples et plus rapides, un environnement plus convivial, un meilleur suivi des procédures, etc. Il ne faut toutefois pas en rester là et l'Observatoire recommande notamment l'élaboration de procédures de consultation pour cerner au plus près les besoins des citoyens et des entreprises. Les citoyens et les entreprises devraient être consultés directement (forum de discussion, sondages, panels représentatifs, etc.) ou indirectement (par le biais d'organisations représentatives), voire être associés aux discussions. Compte tenu de sa composition, l'Observatoire pourrait être l'un des relais entre les acteurs concernés.

3.3. Renforcer la confiance des citoyens et des entreprises dans l'e-gouvernement

Il est nécessaire, pour renforcer la confiance des citoyens et des entreprises dans l'e-gouvernement, d'intervenir simultanément et de façon suffisante dans les domaines suivants : la sécurité, la protection de la vie privée et les bonnes pratiques en matière d'administration électronique. Il est en effet primordial que les autorités publiques aient une vision globale, à moyen ou long terme, de la politique à mener dans ces matières.

3.3.1. Sécurité

Les aspects juridiques et techniques sont indissociables pour assurer la sécurité. Il est souhaitable que certains processus techniques fassent l'objet de dispositions législatives. Par ailleurs, la sécurité ne peut être efficacement garantie sans l'élaboration de procédures de contrôle des dispositifs mis en place.

Trois points peuvent être distingués : au niveau du *front office*, la sécurité contre les attaques extérieures et la sécurité dans les échanges entre l'administration et le citoyen ou l'entreprise et, au niveau du *back office*, la sécurité dans les échanges entre les administrations.

S'agissant de la sécurité vis-à-vis de l'extérieur, des efforts constants doivent être consentis pour garantir un niveau élevé de sécurité, que ce soit en termes techniques ou organisationnels. A cet égard, les pouvoirs publics peuvent s'inspirer des méthodes employées par certaines entreprises et qui ont fait leurs preuves.

Des critères doivent être satisfaits dans certains échanges entre l'administration et les citoyens ou les entreprises, telles l'identification de l'émetteur, l'intégrité du message et la confidentialité de la

communication. Des techniques existent, parfois réglementées par les autorités publiques. La signature électronique permet de rencontrer ces critères, dès lors que diverses conditions sont remplies. Il faut toutefois se garder de l'imposer systématiquement dans tous les échanges. Parfois, l'octroi d'un *login* associé à un mot de passe suffit. Il est donc recommandé d'identifier les procédures pour lesquelles le recours à la signature électronique semble nécessaire (celles qui requièrent que soient respectées l'imputabilité et l'intégrité, par exemple ; cf. art. 1322, al. 2, C. civ.) et de réfléchir à la manière de diffuser cette signature. La généralisation de la carte d'identité électronique, qui serait le support d'un ou de plusieurs certificats, pourrait atteindre cet objectif : la signature électronique se diffuserait par un processus d'engrenage. Par ailleurs, un mandaté devrait être désigné au sein des entreprises pour certaines déclarations (TVA, sécurité sociale), et il serait le seul à pouvoir effectuer ces déclarations.

Les citoyens et les entreprises ne seront rassurés que s'ils savent ce qui est fait des données transmises. Outre une bonne communication (cf. *supra*, point 2, *in fine*) et une réglementation du partage des données entre les administrations (cf. *infra*, point 3.3.2.), il est souhaitable que des procédures de sécurité soient mises en place au sein même de l'administration pour garantir que les destinataires des informations, et eux seuls, reçoivent les données communiquées par les citoyens et les entreprises.

De manière générale, il faut aussi préconiser le chiffrement des données lors de la transmission, ainsi que lors du stockage. Des copies de sauvegarde (*back up*) régulières sont aussi conseillées.

3.3.2. Protection de la vie privée

La protection de la vie privée constitue un principe fondamental de notre droit. Les données à caractère personnel font par ailleurs l'objet d'une réglementation stricte. Les mesures destinées à protéger la vie privée doivent exister, mais elles ne peuvent pour autant rendre les procédures inutilement compliquées. Une telle conséquence irait à l'encontre des objectifs poursuivis par l'e-gouvernement (et notamment la simplification administrative). Les mesures doivent être proportionnelles à l'objectif poursuivi.

Les problèmes en matière de vie privée concernent notamment l'échange des données entre les administrations, l'institution d'un point d'entrée unique ou encore l'attribution d'un identifiant unique⁴. A cet

⁴ Voy. l'article 8, § 7 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 de ces données, *J.O.C.E.*, n° L 281 du 23 novembre 1995 qui prévoit que « Les États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement ».

égard, il est nécessaire d'analyser les risques et d'élaborer des procédures pour y faire face.

S'agissant plus particulièrement de l'échange des données entre les administrations, il faut prévoir des mécanismes de contrôle et de surveillance (autorisation préalable pour l'échange de certains types de données ou cadastre des échanges de données, par exemple). Il faut aussi assurer une transparence suffisante. Il convient d'ailleurs de faire une distinction entre les données consultables librement en raison de leur nature ou de la réglementation existante et les données plus sensibles qui nécessitent une autorisation préalable de consultation. Dans ce contexte, des législations récentes apportent des réponses⁵ : le nouvel article 36 bis de la [loi 8 décembre 1992](#) relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel prévoit en effet la création d'un comité sectoriel au sein de la Commission de la protection de la vie privée et que « sauf dans les cas déterminés par le Roi, 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, exige une autorisation de principe de ce comité sectoriel, à moins que la communication n'ait déjà fait l'objet d'une autorisation de principe d'un autre comité sectoriel créé au sein de la Commission pour la protection de la vie privée ».

3.3.3. Bonnes pratiques dans les relations entre l'administration et les citoyens ou entreprises

Ces bonnes pratiques concernent notamment la gestion des courriers électroniques dans les administrations ainsi que diverses procédures à mettre en œuvre. Pour leur élaboration, les autorités compétentes peuvent utilement s'inspirer des pratiques développées dans d'autres secteurs ou d'autres Etats.

Pour ce qui est de la gestion des courriers électroniques, il faut déterminer par exemple comment gérer ces courriers au sein de l'administration ou dans quelle mesure les réponses fournies engagent l'administration. Le citoyen ou l'entreprise doit aussi être informé de la personne qui, au sein du service compétent, traitera sa demande ou, à tout le moins, en sera responsable.

Quant aux autres procédures à mettre en œuvre, elles doivent rassurer le citoyen ou l'entreprise. On peut ainsi prévoir qu'un accusé de réception est envoyé à l'occasion de toute démarche accomplie et que

⁵ Voy. la [loi du 26 février 2003](#) modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée, *M.B.*, 26 juin 2003, p. 34416.

les coordonnées précises du service chargé du dossier sont indiquées. De même, l'administration doit prendre des mesures raisonnables pour s'assurer de la bonne réception de ses communications par le citoyen. Des procédures techniques doivent être mises en place pour détecter les erreurs dans l'introduction des données et fournir des informations précises et claires en temps opportun. Il faut aussi permettre au citoyen ou à l'entreprise de connaître le suivi de la demande adressée à l'administration.

3.4. Développer le volet transactionnel des services de l'e-gouvernement

A côté de la diffusion d'informations, le développement de l'e-gouvernement peut aussi s'élargir à la fourniture de divers services publics, éventuellement fournis contre rémunération (commande de documents en ligne, par exemple).

Diverses règles pourraient être édictées pour protéger les destinataires du service. Sans se prononcer sur l'application des [lois du 11 mars 2003](#) sur certains aspects des services de la société de l'information⁶ à l'e-gouvernement, l'Observatoire recommande à tout le moins de s'inspirer de certaines de ses dispositions (spécialement les articles 7 et suivants consacrés à l'information, à la transparence et à la publicité). Des progrès pourraient aussi être accomplis sur le thème des paiements des services administratifs. S'il est désormais possible de commander de nombreux documents à travers le *net*, le paiement se fait presque exclusivement par virement bancaire. On pourrait imaginer de généraliser, comme en matière de commerce électronique, les paiements *on line*, en veillant toutefois à offrir au citoyen et à l'entreprise un choix entre divers modes de paiement (*on line* et *off line*).

⁶ M.B., 17 mars 2003.

4. Annexe

Liste des experts ayant apporté une contribution aux travaux du [groupe de travail](#) sur le gouvernement électronique (e-gouvernement).

Membres de l'Observatoire :

- Mme Katia BODARD ([Vrij Universiteit Brussel](#)) ;
- M. Hervé JACQUEMIN ([Centre de Recherches Informatique et Droit](#)) ;
- M. Jan STEENLANT ([Fédération des Entreprises de Belgique](#)) ;
- Mme Caroline VEN ([Fédération des Entreprises de Belgique](#)), coordinatrice du groupe de travail.

Experts :

- M. Georges ATAYA (Consultant) ;
- M. Etienne DAVIO ([Région wallonne](#)) ;
- M. Jan DEPREST ([SPF Technologie de l'Information et de la Communication](#)) ;
- M. Peter GOETHALS ([Communauté flamande](#)) ;
- M. Ewout KEULEERS ([Centre de Recherches Informatique et Droit + ULYS](#)) ;
- Mme Christine MAHIEU ([SPF Technologie de l'Information et de la Communication](#)) ;
- M. Yves POULLET ([Centre de Recherches Informatique et Droit + Commission de la protection de la vie privée](#)) ;
- M. Joseph ROYEN ([Région de Bruxelles-Capitale](#)) ;
- Mme Caroline UYTENDAELE ([Communauté flamande](#)).

Secrétaires :

- M. Markoen DE SMAELE ([SPF Economie, P.M.E., Classes moyennes et Energie](#)), secrétaire de l'Observatoire des Droits de l'Internet ;
- M. Pierre STRUMELLE ([SPF Economie, P.M.E., Classes moyennes et Energie](#)), secrétaire de l'Observatoire des Droits de l'Internet.

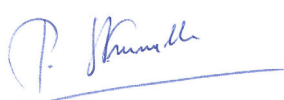
Pour copie certifiée (Bruxelles, le 4/12/2003) :

Les secrétaires,

Le Président,



Markoen DE SMAELE.



Pierre STRUMELLE.



Thibault VERBIEST.

Observatoire des Droits de l'Internet

Site internet

<http://www.internet-observatory.be>

Contacts

Président

Thibault Verbiest

Fax : +32 (0)2 506 63 08

E-mail : president@internet-observatory.be

Secrétariat

Pierre Strumelle (F)

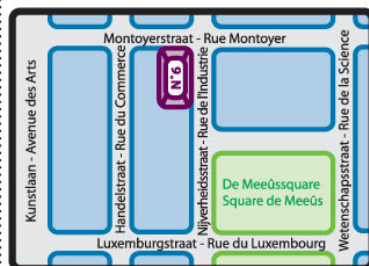
Tél : +32 (0)2 506 63 01

Fax : +32 (0)2 506 63 08

E-mail : secretariat@internet-observatory.be



- 1 Parc de Bruxelles
- 2 Arts-Loi
- 3 Rue de la Loi
- 4 Rue Belliard
- 5 Rue de l'Industrie
- 6 Palais royal
- 7 Trône
- 8 Rue du Trône
- 9 Rue de Luxembourg
- 10 Gare de Bruxelles-Luxembourg



Adresse

Rue de l'Industrie, 6
B - 1000 Bruxelles