Recommandation n° 01/2008 du 24 septembre 2008

Objet : recommandation relative à la gestion des accès et des utilisateurs dans le secteur public (SE/2008/028)

La Commission de la protection de la vie privée (ci-après la "Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la "LVP"), en particulier l'article 30 ;

Vu la demande du Comité sectoriel du Registre national du 12/03/2008 ;

Vu le rapport du Président ;

Émet, le 24/09/2008, la recommandation suivante :

I. OBJET DE LA DEMANDE

1. Lors de la séance du Comité sectoriel du Registre national du 12 mars 2008, une demande d'autorisation émanant de l'Agence flamande de l'Énergie relative à la gestion des utilisateurs d'une banque de données de performances énergétiques a été traitée. Dans le cadre du traitement de ce dossier, le comité sectoriel a constaté que les personnes qui s'enregistreront en vue d'utiliser l'application sont priées de fournir toute une série de renseignements tels que le diplôme, l'orientation du diplôme, la formation suivie, l'adresse de correspondance ou l'information selon laquelle elles sont fonctionnaire dans une commune ou dans un service de l'aménagement du territoire en Flandre, … À l'exception des nom, prénoms et numéro d'identification, ces informations sont ensuite enregistrées dans la banque de données des utilisateurs sans que leur exactitude ait été correctement validée au préalable.

2. Le Comité sectoriel du Registre national a attiré l'attention sur le fait que la constitution de banques de données sans garantie suffisante de l'exactitude des données qui y sont reprises est contraire à l'article 16, § 2, 1° de la LVP qui stipule que "*le responsable du traitement (…) doit faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8*".

3. Lorsque ces banques de données sont utilisées en tant que source fiable pour la vérification de certaines caractéristiques de la personne concernée (par exemple médecin, notaire, …) pour leur donner accès à certaines applications et données à caractère personnel sur la base de ces caractéristiques, certaines personnes risquent de recevoir un accès à des applications ou à des données à caractère personnel sur la base de caractéristiques incorrectes. Qu'est-ce qui empêche par exemple une personne de s'attribuer une caractéristique qu'elle n'a pas, par exemple prestataire de soins, si cet élément n'est de toute façon pas contrôlé ?

4. Le risque existe en outre que de telles banques de données reçoivent un cachet officiel et que d'autres instances y recourent, en partant du principe, à tort, qu'elles sont fiables parce qu'elles sont gérées par un service public, avec toutes les conséquences que cela implique. Ainsi, il serait possible qu'une personne ait indûment accès à des données en vertu d'une qualité fictive. Par conséquent, il importe de fixer un certain nombre de règles pratiques devant être respectées dans le cadre du développement d'un système de gestion des utilisateurs et des accès afin d'éviter de tels excès.

5. Vu qu'il s'agit d'une problématique horizontale qui dépasse la compétence du Comité sectoriel du Registre national, il a été décidé de recueillir le point de vue de la Commission à cet égard.

II. ANALYSE

A. Généralités

6. Avec le service électronique, il est notamment possible d'accéder à des informations personnelles et/ou éventuellement sensibles, ou d'effectuer des actions ayant des conséquences (juridiques). Il est dès lors crucial que seules des personnes et/ou organisations habilitées disposent d'un accès et qu'elles ne puissent consulter que les informations auxquelles elles sont autorisées à accéder ou qu'elles ne puissent effectuer que les actions pour lesquelles elles ont reçu une autorisation. Ceci requiert l'élaboration d'un système fiable de gestion des utilisateurs et des accès qui détermine quel utilisateur/quelle application peut accéder en quelle qualité et dans quelle situation à quels types de données relatifs à quelles personnes et pour quelle période.

7. Comme le terme l'indique, la gestion des utilisateurs et des accès se compose de 2 volets. La gestion des utilisateurs qui comprend les aspects suivants :

- l'enregistrement de l'identité ;
- l'identification ;
- l'authentification de l'identité ;
- l'enregistrement des caractéristiques et des mandats ;
- la vérification des caractéristiques et des mandats ;

et la gestion des accès qui couvre l'enregistrement des autorisations et la vérification de ces dernières.

8. Au sein du secteur public (fédéral, communautaire, régional, administrations locales, …), la Commission préconise un système bien coordonné de gestion des utilisateurs et des accès basé sur la carte d'identité électronique comme moyen d'identification et d'authentification de l'identité et sur la constitution de banques de données authentiques validées et distribuées (ce qu'on appelle les sources authentiques) pour l'enregistrement et la vérification de caractéristiques, de mandats et d'autorisations. Au sein des pouvoirs publics, il est souhaitable de conclure des accords afin qu'une seule banque de données authentique validée soit constituée pour chaque caractéristique, mandat et autorisation pertinents. Cela évite les risques relatifs à la protection de la vie privée qui sont propres à l'enregistrement redondant des mêmes données à caractère personnel dans plusieurs banques de données authentiques et cela épargne aux utilisateurs de devoir prouver à plusieurs reprises les mêmes caractéristiques ou mandats. Cela signifie que les banques de données authentiques validées

feront partie des services de base sur lesquels peut se fonder chaque gestion des utilisateurs et des accès, moyennant éventuellement une autorisation du comité sectoriel compétent.

9. Il est préférable d'élaborer le système selon le principe des "cercles de confiance". Cela implique que des accords clairs soient conclus entre les instances participant au service électronique, sur :

- qui effectue quelles authentifications, quelles vérifications et quels contrôles à l'aide de quels moyens et qui en est responsable ;
- la manière dont les résultats des authentifications, vérifications et contrôles effectués sont échangés de manière sûre par voie électronique entre les instances concernées ;
- qui tient à jour quels loggings ;
- la manière dont on veille à ce que puisse avoir lieu, lors d'un examen effectué à l'initiative d'un organe de contrôle ou à l'occasion d'une plainte, un traçage complet (qui, quoi, où, quand, pourquoi) de la personne physique qui a utilisé quel service ou quelle transaction concernant quel citoyen ou quelle entreprise, quand, via quel canal et pour quelles finalités.

Les avantages d'un tel système sont les suivants :

- on évite une centralisation inutile ;
- on évite des menaces inutiles pour la protection de la vie privée (par exemple, aucune copie des sources authentiques validées ne va circuler) ;
- on évite de multiples contrôles identiques et l'enregistrement des loggings ;
- on travaille avec les informations les plus actuelles (par exemple lorsqu'un utilisateur perd une caractéristique, au moment de se présenter, il sera traité de manière appropriée par le système).

B. Terminologie

10. Pour une bonne compréhension, nous allons préciser les termes utilisés dans ce contexte afin qu'il n'y ait aucun malentendu sur leur portée :

- l'identité de l'utilisateur est un numéro unique ou une série d'attributs d'un utilisateur (personne physique, entreprise, établissement d'une entreprise, …) qui permettent de savoir sans équivoque qui est l'utilisateur. Cela implique qu'un utilisateur a une et une seule identité. Le fait qu'un pseudonyme puisse éventuellement être utilisé dans certaines situations n'y change rien ;

- une caractéristique est un attribut d'un utilisateur, différent des attributs qui déterminent l'identité de l'utilisateur, comme une qualité, une fonction dans une certaine organisation, une qualification professionnelle, … Un utilisateur peut avoir différentes caractéristiques ;

- un mandat est un droit octroyé par un utilisateur identifié à un autre utilisateur identifié afin qu'il puisse effectuer des actions (juridiques) déterminées en son nom et pour son compte. Un utilisateur peut octroyer un ou plusieurs mandats à un ou plusieurs utilisateurs ;

- l'enregistrement est le processus par lequel l'identité d'un utilisateur, une caractéristique d'un utilisateur ou un mandat est déterminé avec suffisamment de certitude avant la mise à disposition de moyens à l'aide desquels l'identité, une caractéristique ou un mandat peuvent être authentifiés ou vérifiés ;

- l'authentification de l'identité est le processus par lequel on vérifie si l'identité qu'un utilisateur prétend avoir est l'identité correcte pour pouvoir utiliser un service électronique. Ceci peut se faire sur la base d'un contrôle de :
    - connaissances (par exemple, un mot de passe) ;
    - détention (par exemple un certificat sur une carte lisible électroniquement) ;
    - propriété(s) biométrique(s) ;
    - une combinaison de plusieurs de ces moyens.

- la vérification d'une caractéristique ou d'un mandat est le processus par lequel on vérifie si une caractéristique ou un mandat qu'un utilisateur prétend avoir pour pouvoir utiliser un service électronique est effectivement une caractéristique ou un mandat de cet utilisateur. Cela peut se faire :
    - sur la base du même type de moyens que ceux utilisés pour l'authentification de l'identité ;
    - après authentification de l'identité d'un utilisateur, en consultant une banque de données (source authentique) où sont enregistrés les caractéristiques ou les mandats relatifs à un utilisateur identifié.

- l'autorisation est la permission, pour un utilisateur, d'effectuer un traitement déterminé ou d'utiliser un service déterminé.

C. Quant au fond

11. Lors de l'élaboration de la gestion des utilisateurs, un bon enregistrement de l'identité, des caractéristiques pertinentes et des mandats pertinents est crucial. Tout est lié à la qualité de cet enregistrement. Un enregistrement de qualité suppose en outre que les données disponibles soient tenues à jour. C'est une évidence. Une modification d'une caractéristique/d'un mandat d'un utilisateur peut en effet avoir des répercussions sur les droits d'accès de ce dernier.

12. Un bon enregistrement implique que l'identité de l'utilisateur qui se manifeste, ses caractéristiques et ses mandats soient contrôlés à l'aide de documents/sources authentiques lorsque cela est possible.

13. Ensuite, il faut déterminer à l'aide de quel instrument on procèdera à une vérification lorsqu'une personne se présente pour utiliser un service électronique avec qui ce service a à voir : identification de l'utilisateur et contrôle pour s'assurer que cette personne est bien celle qu'elle prétend être.

14. La Commission estime que l'authentification électronique de l'identité doit se faire de préférence à l'aide de la carte d'identité électronique (eID) car elle offre le maximum de garanties. Elle combine la détention d'un document spécifique avec la connaissance d'une information déterminée (code PIN). En outre, un certain nombre de facteurs matériels et légaux limitent le risque d'abus en cas de perte/vol éventuel de la eID :

- il s'agit d'un document officiel légalement protégé qui est délivré par les pouvoirs publics ;
- l'absence de la eID sera plus rapidement remarquée par son titulaire légitime que celle d'autres cartes généralement utilisées uniquement sporadiquement ;
- sans le code PIN, on ne peut rien entreprendre électroniquement avec la carte ;
- sur la base de l'article 6*ter* de la loi du 19 juillet 1991 *relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques*, en cas de perte/de vol, les fonctions électroniques de la carte peuvent à tout moment du jour ou de la nuit être suspendues ou retirées en déclarant la perte / le vol au helpdesk du Registre national des personnes physiques[1].

[1] Ce helpdesk est opérationnel vingt-quatre heures sur vingt-quatre, sept jours sur sept (article 7 de l'arrêté royal du 25 mars 2003 *relatif aux cartes d'identité*).

15. Le fait que l'identité d'un utilisateur ait été authentifiée ne suffit pas toujours pour octroyer à la personne concernée un accès, sans autre condition, à un service électronique. Les droits d'accès à un service électronique (autorisations) dont bénéficie un utilisateur dans le cadre du service électronique peuvent être liés à ses caractéristiques et/ou à ses mandats. Une gestion tout à fait intégrée des utilisateurs et des accès exige donc que puissent être contrôlées sans équivoque :

- les caractéristiques pertinentes d'une personne ;
- l'existence d'un mandat entre une personne morale ou physique à laquelle se rapporte un service électronique et la personne qui utilise ce service.

16. La vérification des caractéristiques et/ou des mandats ne pourra pas être effectuée à l'aide de la eID étant donné qu'outre le fait d'être un instrument permettant d'apposer une signature électronique juridiquement valable, elle constitue exclusivement un instrument d'identification et d'authentification de l'identité. Cela signifie que les informations contenues sur cette carte, que ce soit sous une forme lisible électroniquement ou visible à l'œil nu, sont limitées et doivent le rester :

- aux informations nécessaires à l'identification du titulaire ;
- aux certificats (clés) qui permettent au titulaire de s'authentifier, c'est-à-dire qui lui permettent de prouver qu'il est effectivement celui qu'il prétend être ;
- aux certificats (clés) qui permettent au titulaire d'apposer une signature électronique juridiquement valable.

Les données qui n'ont rien à voir avec l'identification et l'authentification d'une personne physique ou avec la signature électronique, comme les caractéristiques et/ou les mandats, n'ont pas leur place sur la eID[2].

17. La vérification de caractéristiques et/ou de mandats devra donc être effectuée via d'autres canaux. Il n'est pas souhaitable de se fier à cet égard à des informations non validées, qui sont tout simplement fournies par l'utilisateur lui-même. Ces éléments doivent être contrôlés à l'aide d'une source qui offre les garanties nécessaires en matière d'exactitude et d'actualité des informations qu'elle contient, une source authentique validée. Le gestionnaire d'une telle source authentique validée est responsable de la disponibilité et de la qualité des informations mises à disposition.

[2] Voir avis de la Commission n° 13/2005 du 7 septembre 2005.

18. Un facteur critique de succès d'une bonne gestion électronique des utilisateurs et des accès est notamment la mesure dans laquelle il est possible de retourner aux sources authentiques validées. Il est dès lors évident que celui qui souhaite élaborer un tel système de gestion doit savoir à quelles sources il peut recourir. Cela requiert la disponibilité d'un inventaire des sources authentiques validées.

19. Cela signifie que tant au niveau fédéral que régional, notamment les services publics et apparentés qui disposent d'informations fiables qui révèlent des caractéristiques ou des mandats d'une personne doivent être identifiés. En outre :

- les informations authentiques doivent être répertoriées ;
- les éléments qui révèlent la qualité de la personne doivent être indiqués ;
- ces informations doivent être organisées de manière à pouvoir facilement être divulguées en respectant le principe de proportionnalité.

20. La Commission est bien consciente du fait que ceci n'est pas simple. Toutefois, si l'on veut développer l'e-government de manière sûre, il s'agit d'un exercice nécessaire. D'ailleurs, en vue de l'application de la Directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 *relative aux services dans le marché intérieur* (la dite "directive services"), cet exercice semble quoi qu'il en soit souhaitable.

21. La 'directive services' vise en effet à simplifier les procédures et les formalités d'accès et d'exercice d'activités de services, à permettre aux prestataires de services qui le souhaitent de régler ces procédures et ces formalités à distance par voie électronique et/ou via un seul guichet, et à offrir à distance des informations accessibles, claires, conviviales et actuelles aux prestataires de services et aux clients de ces services. Cela implique que les états membres s'entraident pour garantir le contrôle des prestataires de services et de leurs services. À cet effet, la Commission européenne a conçu un système d'information pour le marché intérieur (IMI). Ce système permettra d'obtenir, via un point de liaison, des informations sur la réalité de l'établissement, la fiabilité et les compétences professionnelles du prestataire de services.

22. Actuellement, au niveau fédéral, un certain nombre de banques de données qualifiées de source authentique validée sont opérationnelles. Pensons par exemple à la Banque-carrefour des Entreprises, à la banque de données de gestionnaires locaux d'entreprises, de communes et de CPAS au sein de l'ONSS(APL), au cadastre des prestataires de soins du SPF Santé publique, à la banque de données des agréments INAMI de l'INAMI. Pour un certain nombre de professions réglementées, des banques de données authentiques validées sont également disponibles. Pensons

par exemple aux avocats, aux notaires, aux huissiers de justice. Au niveau régional et local aussi, de telles banques de données sont disponibles.

23. Lorsqu'un système de gestion d'utilisateurs et d'accès est mis sur pied, le prestataire de services concerné doit vérifier pour quels éléments il peut se référer à des sources qui peuvent actuellement déjà être qualifiées de source authentique validée. Si tel est le cas, il doit prendre les dispositions nécessaires pour les intégrer dans son système en tant que service de base.

24. À défaut d'une source authentique validée relative à certaines caractéristiques et/ou mandats, il doit vérifier si, à cet égard, aucune information n'est disponible auprès d'un tiers qui peut, sous certaines conditions, recevoir le cachet de source authentique validée. Souvent, un tiers dispose d'informations fiables mais celui-ci n'est pas connu et par conséquent, on ne recourt pas à lui. Le détenteur de ces informations ne va dès lors pas faire d'efforts pour les divulguer.

25. Comme le concept l'indique, le dernier maillon de la gestion des utilisateurs et des accès est la gestion des accès. Celle-ci consiste en l'enregistrement et la vérification des autorisations où :

- l'enregistrement implique l'introduction d'autorisations dans une source authentique par le fournisseur du service électronique, avec spécification des traitements qui peuvent être effectués concernant quels services et sous quelles conditions (par exemple caractéristiques, mandats, …) pendant quelle période. Certains utilisateurs (exemple les gestionnaires locaux) peuvent en outre octroyer les autorisations qui leur ont été accordées à des utilisateurs qu'ils désignent en introduisant des autorisations dans une source authentique ;
- la vérification implique la consultation des sources authentiques d'autorisations pertinentes.

26. Une gestion des utilisateurs et des accès élaborée en tenant compte des directives exposées ci-dessus contribuera à limiter le risque d'octroyer un accès non autorisé par voie électronique à des informations ou que ne soient effectuées des actions non autorisées.

PAR CES MOTIFS,

la Commission recommande que :

↳ lors de l'organisation de la gestion des utilisateurs et des accès, les points suivants soient pris en considération :

- l'enregistrement scrupuleux de l'identité, des caractéristiques et des mandats ;

- l'utilisation de la eID exclusivement pour l'identification et l'authentification de l'identité, pas pour des caractéristiques et des mandats ;
- le contrôle des caractéristiques et des mandats à l'aide d'une source authentique validée ;
- la mise en place de cercles de confiance ;
- l'enregistrement des autorisations dans une source authentique.

↳ la ou les autorité(s) compétente(s) prend (prennent) des initiatives afin de dresser l'inventaire des sources authentiques validées existantes ainsi que des sources qui peuvent entrer en considération à cet effet sous certaines conditions en vue de développer un e-government fiable et sûr.

Pour L'Administrateur e.c., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere