Avis n° 12/2009 du 29 avril 2009

Objet : demande d'avis émanant du SPF Intérieur concernant un certain nombre de questions qui se sont posées dans le cadre de la délibération RN n° 19/2008 (A/2009/007)

La Commission de la protection de la vie privée ;

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 29 ;

Vu la demande d'avis de Monsieur Guido DE PADT, Ministre de l'Intérieur, reçue le 06/03/2009 ;

Vu le rapport de Monsieur Frank SCHUERMANS ;

Émet, le 29 avril 2009, l'avis suivant :

I. ANTÉCÉDENTS

1. Le 28 avril 2008, le Service public fédéral Technologie de l'Information et de la Communication (Fedict) a introduit auprès du Comité sectoriel du Registre national une demande pour être autorisé à accéder aux informations du Registre national et à utiliser le numéro d'identification de ce registre en vue de tester, corriger et entretenir des applications informatiques qui ont une connexion avec le Registre national via l'UME, le FSB et les Web Services[1].

2. Par la délibération RN n° 19/2008 du 7 mai 2008, le Comité sectoriel du Registre national a octroyé l'autorisation demandée aux conditions suivantes :

a. avant de procéder aux activités internes de test, de correction et d'entretien, le conseiller en sécurité de Fedict détermine la population qui peut faire l'objet de tests ;
b. cette population comprend un maximum de 10.000 personnes ;
c. le conseiller en sécurité contrôle scrupuleusement le respect de ces paramètres par les personnes qui effectuent concrètement ces activités ;
d. les résultats des tests sont conservés au maximum 1 an dans un environnement sécurisé ;
e. les logs des activités de test sont conservés au minimum 10 ans ;
f. les applications de Fedict doivent uniquement être authentifiées vis-à-vis du Registre national à l'aide d'un certificat d'application, donc sans que l'identité de l'utilisateur final doive être communiquée au Registre national.

3. Cette délibération est manifestement problématique pour le Service public fédéral Intérieur parce qu'elle remettrait en question le rôle et les missions du Registre national en tant que gestionnaire de l'identité électronique en Belgique et d'intermédiaire dans l'échange d'informations liées à l'identité. Elle hypothéquerait également l'obligation de transparence prévue à l'article 6, § 3, 3° 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*.

[1] L'UME (Universal Messaging Engine) est l'instrument qui a été conçu par Fedict pour permettre des communications avec et entre les différents systèmes de l'autorité fédérale, au moyen de messages standardisés. L'UME a évolué vers le FSB (Federal Service Bus). Ce FSB fonctionne de manière encore plus intelligente que l'UME lors du traitement de messages, simplifiant encore, pour les fonctionnaires et les entreprises compétents, l'approche des différentes applications informatiques et des différents fichiers de données de l'autorité fédérale. Les Web Services permettent de réclamer à un serveur un service à distance (généralement via Internet) au départ d'un ordinateur d'un client, par exemple la fourniture de données.

4. Faisant suite à cela, le Service public fédéral Intérieur souhaite connaître la position (l'avis) de la Commission concernant 3 points problématiques, à savoir :

- le rôle et les responsabilités dans le cadre de la gestion de l'identité électronique en Belgique ;
- l'obligation de transparence ;
- la finalité pour laquelle une autorisation a été accordée.

II. QUANT AU FOND

2.1. Remarque préalable

5. La Commission souhaite remarquer au préalable qu'elle ne peut se défaire de l'idée que la demande d'avis l'incite à endosser le rôle d'instance de recours pour des décisions prises par un des comités sectoriels. Ce n'est aucunement prévu réglementairement et la Commission n'a pas du tout l'intention de remplir un tel rôle.

6. S'il y a des questions concernant une délibération, il est recommandé d'en discuter en premier lieu avec le comité sectoriel concerné.

7. Toutefois, la Commission peut difficilement ne pas tenir compte d'une demande d'avis et s'est par conséquent penchée sur les questions soumises.

2.2. Rôle et responsabilités dans le cadre de la gestion de l'identité électronique en Belgique

8. Le Service public fédéral Intérieur fait remarquer que Fedict évolue vers une plate-forme intermédiaire et un intégrateur de services. L'octroi de telles compétences sur la base d'une simple autorisation du Comité sectoriel du Registre national est contraire aux dispositions constitutionnelles et légales protectrices de la vie privée.

9. On ne peut pas nier qu'il y ait de fortes chances en effet que Fedict endosse avec le temps le rôle d'intégrateur de services. Il est incontestable que cela requiert un cadre légal. Un projet de loi est d'ailleurs en préparation à cet effet. Le 24 octobre 2008, l'avis de la Commission a été demandé

concernant un avant-projet de loi relative à l'institution et à l'organisation d'un Intégrateur de Services fédéral[2].

10. L'autorisation susmentionnée du Comité sectoriel du Registre national a été octroyée en tenant compte de :

- l'article 5, premier alinéa, 1° de la loi du 8 août 1983 *organisant un Registre national des personnes physiques* (ci-après la "LRN"), en vertu duquel une autorisation peut être accordée aux autorités publiques belges pour les informations qu'elles sont habilitées à connaître en vertu d'une loi, d'un décret ou d'une ordonnance ;

- l'article 5, deuxième alinéa de la LRN qui subordonne un accès à une finalité déterminée, explicite et légitime et stipule en outre que cet accès doit être limité à des données pertinentes et non excessives par rapport à ces finalités ;

- l'article 5, troisième alinéa de la LRN qui stipule qu'il faut vérifier si la communication est conforme à la LVP ;

- l'arrêté royal du 11 mai 2001 *portant création du Service public fédéral Technologie de l'Information et de la Communication* qui définit l'ensemble actuel de tâches de Fedict.

11. Une des missions de Fedict consiste à développer l'architecture de base pour une mise en œuvre efficace de la technologie de l'information et de la communication à l'appui de la stratégie commune en matière d'e-government et à en surveiller le respect (article 2, § 1, 4° de l'arrêté royal du 11 mai 2001). En exécution de cette disposition, Fedict a développé un UME, un FSB et des Web Services qui sont mis à la disposition des autorités fédérales afin qu'elles puissent échanger des messages électroniques. Le but est donc que des instances dûment habilitées puissent disposer d'un accès au Registre national via cette voie.

12. La délibération critiquée précise à juste titre ce qui suit : "*L'élaboration de telles applications ne constitue toutefois pas en soi une garantie d'un service de qualité. Ce n'est qu'après des tests concluants – ce qui implique éventuellement certaines corrections – qu'une application peut être mise en production. Il faut ensuite assurer l'entretien de l'application. Tout ce processus, essentiel au développement de projets d'e-government, s'inscrit dans le cadre des missions réglementaires du demandeur.*"

---

[2] La Commission a émis un avis positif n° 41/2008 le 17 décembre 2008.

13. L'autorisation a donc été accordée en vue d'une finalité déterminée qui trouve son fondement dans un arrêté royal en vigueur. L'affirmation selon laquelle, par la délibération RN n° 19/2008, le Comité sectoriel du Registre national confère à Fedict la qualité d'intégrateur de services est donc inexacte. Les autres commentaires que le Service public fédéral Intérieur formule à l'égard de la problématique "intégrateur de services" ne sont dès lors pas pertinents.

14. La Commission pense pouvoir déduire du courrier du Service public fédéral Intérieur que l'institution d'un intégrateur de services fédéral est perçue par le Service public fédéral comme une menace pour la sécurité et la transparence des données et des flux de données.

15. La Commission estime que cette crainte n'est pas fondée. L'intervention d'un intégrateur de services a normalement une influence positive sur la sécurité des données et des flux de données. La transparence n'est pas non plus compromise, à condition que les accords nécessaires soient conclus et que les mesures organisationnelles nécessaires soient prises.

16. La Commission renvoie à cet égard aux principes exposés dans sa recommandation n° 01/2008 du 24 septembre 2008 *relative à la gestion des accès et des utilisateurs dans le secteur public*. Elle émettra d'ailleurs un avis relatif à l'intégration de services lors d'une de ses prochaines séances.

17. Ces principes, associés à un cadre législatif, offrent des garanties suffisantes en matière de transparence et de sécurité.

2.3. Obligation de transparence

18. L'article 6, § 3, 3° de la loi du 19 juillet 1991 stipule que le titulaire d'une carte d'identité électronique (eID) peut, au moyen de cette carte, "*connaître toutes les autorités, organismes et personnes qui ont, au cours des six mois écoulés, consulté ou mis à jour ses données au registre de la population ou au Registre national des personnes physiques (…)*".

19. Le fait que des applications soient authentifiées vis-à-vis du Registre national à l'aide d'un certificat d'application signifie, selon le Service public fédéral Intérieur, que :

- la transparence introduite par l'article 6, § 3, 3° de la loi du 19 juillet 1991 est remise en question parce qu'il n'est pas jugé nécessaire que le Registre national conserve les données permettant d'identifier l'utilisateur final ;
- l'utilisation de la eID comme instrument d'authentification est remise en cause.

20. La discussion relative à la portée de l'article 6, § 3, 3° de la loi du 19 juillet 1991 n'est pas nouvelle. La Commission s'est déjà penchée sur ce problème en séance du 8 février 2006 et a communiqué son point de vue à cet égard au Service public fédéral Intérieur par courrier du 24 février 2006. Ce point de vue est toujours d'actualité. Toutefois, il ne s'agissait que d'une communication bilatérale. C'est pourquoi il est bon de rappeler ici les éléments suivants, pour bien comprendre le problème.

"***Portée du terme "personne"***

L'article 6, § 3, 2ème alinéa, 3°, de la loi du 19 juillet 1991 stipule en effet que le titulaire d'une carte d'identité a le droit de "connaître toutes les autorités, organismes et personnes qui ont, au cours des six mois écoulés, consulté ou mis à jour ses données au registre de la population ou au Registre national des personnes physiques (...)". Cette terminologie a également été adoptée dans l'arrêté royal déterminant la date d'entrée en vigueur et le régime du droit de prendre connaissance des autorités, organismes et personnes qui ont consulté ou mis à jour les informations reprises dans les registres de population ou au Registre national des personnes physiques qui a été pris le 13 février 2005 en exécution dudit article.

La Commission estime que les mots "autorités, organismes et personnes" utilisés dans l'article précité sont inspirés par l'article 5 de la loi du 8 août 1983 et les instances pouvant être autorisées, en application de celui-ci, à accéder aux informations du Registre national ou à en obtenir communication, instances qui sont – en termes généraux – des autorités, des organismes et des personnes (physiques ou morales).

L'autorisation délivrée sur la base de l'article 5, 1er alinéa, 3°, de la loi du 8 août 1983 peut aussi bien l'être à des personnes physiques qu'à des personnes morales, pour autant qu'elles agissent en qualité de sous-traitant. C'est à cette catégorie de titulaires d'une autorisation que fait référence l'expression "personnes" utilisée à l'article 6, § 3, 2ème alinéa, 3°, de la loi du 19 juillet 1991. Dès lors, si le titulaire d'une autorisation au nom duquel une consultation est effectuée relève de la catégorie précitée, le nom de la personne physique ou celui de la personne morale sera mentionné.

Pour en arriver à cette conclusion, la Commission se base sur les finalités sous-jacentes de cette disposition, à savoir, d'une part, préserver au mieux la vie privée – ce qui implique notamment que tout citoyen ait la possibilité d'apprendre qui a consulté ses données (transparence, obligation d'information) – et, d'autre part, permettre au citoyen de jouer un rôle d'avertisseur – puisqu'il est le mieux placé pour détecter des consultations "anormales" pouvant donner lieu à des sanctions.

La Commission constate que le citoyen ne peut tirer aucune conclusion quant au motif et à la régularité d'une consultation sur la seule base du nom du fonctionnaire ayant effectué celle-ci. Dès lors, compte tenu des finalités précitées, la communication du nom de l'agent doit être considérée comme excessive au regard de l'article 4, § 1, 3°, de la LVP.

Le droit reconnu au citoyen de savoir par qui ses données ont été consultées est intégralement rencontré si l'identité du titulaire d'une autorisation au nom duquel la consultation a été effectuée lui est communiquée. Pour connaître le motif d'une consultation ou pour pouvoir porter un jugement sur sa régularité, il faut de toute façon toujours prendre contact avec celui qui est (juridiquement) responsable, c'est-à-dire le titulaire de l'autorisation. En effet, il est indispensable que celui-ci puisse justifier pourquoi son préposé a consulté les données d'une personne déterminée à une certaine date. Ceci implique que le titulaire de l'autorisation démontre :

- *qu'il est en charge d'un dossier relatif à la personne concernée ;*
- *que la consultation des données de l'intéressé a eu lieu dans le cadre de la gestion dudit dossier, conformément aux modalités de l'autorisation.*

Il importe donc que le citoyen, s'il a des questions à poser, sache, sur la base de la liste des instances ayant consulté ses données, à qui il doit s'adresser pour obtenir des explications détaillées. C'est le titulaire de l'autorisation qui est le mieux placé pour cela, vu son savoir-faire. L'attention est attirée sur le point suivant : une consultation effectuée par un détenteur d'autorisation auprès duquel le citoyen n'a pas de dossier en cours n'est pas ipso facto irrégulière. Pour illustrer ce qui précède, on peut citer l'exemple d'une recherche phonétique dans le Registre national. Les données de toutes les personnes apparaissant dans la liste des occurrences seront contrôlées en vue de trouver celle effectivement concernée par un dossier dont le titulaire de l'autorisation a la charge. C'est ce dernier qui doit expliquer de manière intelligible au citoyen que ses données ont été contrôlées dans le cadre du processus d'élimination résultant d'une recherche phonétique effectuée dans le contexte d'un dossier déterminé.

Dans cette perspective, la Commission estime que la seule mention du titulaire de l'autorisation, par exemple le SPF Justice, n'est pas assez précise. Pour que le citoyen puisse se tourner directement vers le bon interlocuteur, il est nécessaire de mentionner de façon précise celui des services du titulaire de l'autorisation au départ duquel la consultation est intervenue, ainsi que la "personne de contact" à laquelle on peut s'adresser pour obtenir davantage d'informations. Celle-ci est tenue de fournir à la personne concernée les coordonnées du responsable du traitement visé, ou de son préposé à la protection des données, ainsi que des informations complémentaires à ce sujet

(finalités, ...), de manière à ce que la volonté du législateur d'assurer une protection supplémentaire aux personnes concernées se réalise effectivement dans la pratique.

Ce point de vue ne signifie nullement qu'un employé peut impunément mésuser de l'accès au Registre national.

Le titulaire d'une autorisation est responsable du bon usage de celle-ci. C'est donc à lui qu'il revient en premier lieu de veiller à ce que ses employés ne l'utilisent pas de manière abusive. Il doit par conséquent disposer d'un système détaillé de "logins" s'étendant jusqu'aux individus (voir aussi le point 6 du document "Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel" rédigé par la Commission).

Un tel système est indispensable. Grâce à lui, le titulaire de l'autorisation lui-même est en mesure d'agir de manière proactive, par exemple en cas d'augmentation anormale du nombre de consultations effectuées par un de ses employés. Il lui permet également de contrôler, de son propre chef et à intervalles réguliers, l'accès de ses employés. En un mot, si des éclaircissements sont demandés, par un citoyen ou en son nom, à propos d'une consultation déterminée, ce système constitue l'instrument idéal pour fournir à l'intéressé des explications détaillées à ce sujet (se justifier).

Si une consultation se révèle irrégulière, l'employé fautif pourra être identifié et se voir demander des comptes, que ce soit suite à une procédure de plainte devant la Commission ou à la suite d'une procédure judiciaire.

Le fait de savoir que leur accès aux données est enregistré incitera les employés à en faire bon usage, étant donné qu'ils seront le cas échéant appelés à se justifier à ce propos (cela contribuera à juguler des pratiques courantes telles que confier son mot de passe à des collègues).

Modalités pratiques de la réalisation de ce droit

Concernant les modalités d'exécution qui doivent être accordées en pratique au droit de consultation électronique consacré à l'article 6, § 3, alinéa 2, 3° de loi précitée du 19 juillet 1991, l'article 2 de l'A.R. du 13/02/2005[3] prévoit que ce droit s'exerce "au moyen d'un appareil de lecture relié à un ordinateur connecté à Internet et par l'intermédiaire du site Internet du Registre national."

---

[3] AR du 13 février 2005 déterminant la date d'entrée en vigueur et le régime du droit de prendre connaissance des autorités, organismes et personnes qui ont consulté ou mis à jour les informations reprises dans les registres de population ou au registre national des personnes physiques, M.B. 28-02-2005.

La Commission considère que, lorsqu'un citoyen s'interroge sur les destinataires de ses données à caractère personnel, ce citoyen doit pouvoir s'adresser au gestionnaire desdites données à caractère personnel. En d'autres termes, si la question concerne les données à caractère personnel conservées par le Registre national, tout citoyen doit adresser sa demande audit registre national (y compris si le destinataire desdites données en a obtenu l'accès non directement des services du Registre national mais de façon indirecte par le truchement d'une organisation intermédiaire). Ce principe résulte de l'article 10 de la LVP et de ses modalités d'exécution prévues dans l'AR de 2001.

Outre les termes de l'article 2 précité, la Commission renvoie au principe de droit administratif de séparation des administrations, au fait que les services du Registre national sont sous la responsabilité ministérielle du Ministre de l'Intérieur et au fait que des organisations intermédiaires qui accèdent au Registre national pour communiquer lesdites informations du Registre national à d'autres organismes peuvent dépendre le cas échéant d'un autre ministre que celui de l'Intérieur.

Les services du Registre national conservent eux-mêmes les informations relatives au destinataire d'une consultation directe.

S'il est question d'une consultation indirecte (par exemple via la banque-carrefour de la sécurité sociale), la question suivante se pose : les informations se rapportant au destinataire final doivent-elles également être conservées par les services du Registre national ?

La Commission constate que l'article 6, § 3 de la loi de 1991 précitée et son Arrêté Royal d'exécution précité ne l'imposent pas.

Pour le citoyen, l'important est d'obtenir les informations demandées et que celles-ci soient correctes.

La Commission est d'avis qu'il ne s'impose pas que les services du Registre national, dans ces hypothèses, reçoivent les "fichiers logs" de connexion des serveurs d'une organisation intermédiaire et conservent l'identité des destinataires finaux desdites données du registre national ; il peut être noté que ces services pourraient, de cette manière, avoir accès à des informations sensibles sur les personnes concernées telles que, par exemple, le nom de la mutuelle à laquelle une personne est affiliée.

À l'occasion d'une demande d'une personne concernée visant à prendre connaissance des consultations de ses données à caractère personnel effectuées au Registre national, il peut

apparaître que certaines de ces consultations ont été effectuées via un organisme intermédiaire. Dans ces cas, il est envisageable de renvoyer le citoyen auprès de cet organisme intermédiaire, au moyen par exemple d'un hyperlien, afin que ce dernier lui communique les informations demandées dans le cadre l'article 6, § 3, alinéa 2, 3° de la loi du 19 juillet 2001.

Dans cette mesure, la Commission est d'avis que les citoyens doivent adresser leur demande de consultation aux services du Registre national et que les réponses auxdites demandes peuvent, le cas échéant, être fournies par un organisme tiers."

21. Cette lecture et cette application de l'article 6, § 3, deuxième alinéa, 3° de la loi du 19 juillet 1991 correspondent parfaitement aux principes suivant lesquels la gestion des accès et des utilisateurs est organisée (recommandation n° 01/2008) et aux principes suivant lesquels l'intégration de services doit être organisée.

22. Il est inexact d'affirmer que le point de vue du Comité sectoriel du Registre national et de la Commission privilégierait l'utilisation de systèmes d'authentification de moindre qualité au détriment de la eID en tant qu'instrument d'authentification. L'utilisation d'une application qui s'authentifie vis-à-vis du Registre national à l'aide d'un certificat d'application est nécessairement associée à une gestion des accès et des utilisateurs. À cet égard, le point 14 de la recommandation n° 01/2008 stipule explicitement que : "*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)*."

23. En résumé, la Commission estime donc que :

- l'intervention d'un ou de plusieurs intégrateurs de services ne compromet pas la transparence prévue à l'article 6, § 3, deuxième alinéa, 3° de la loi du 19 juillet 1991 ;
- l'article susmentionné ne comporte aucune obligation, dans le chef du Registre national, d'enregistrer lui-même les informations relatives à l'utilisateur final ;
- le fait de travailler avec des applications qui s'authentifient vis-à-vis du Registre national à l'aide d'un certificat d'application ne décourage nullement l'utilisation de l'eID en tant qu'instrument d'authentification, au contraire.

2.4. Finalité pour laquelle l'autorisation a été accordée et accès à l'environnement de production

24. Ce titre reprend les remarques formulées par le Service public fédéral Intérieur concernant la finalité pour laquelle l'autorisation a été accordée, la proportionnalité de l'accès et le délai de conservation des données.

25. La Commission attire l'attention sur le fait que le Comité sectoriel du Registre national dispose d'une compétence d'appréciation souveraine concernant ces points et qu'il n'appartient pas à la Commission de se substituer à l'un de ses comités sectoriels dans ce domaine.

26. Par souci d'exhaustivité, la Commission attire l'attention à ce sujet sur les points suivants.

27. Il ressort de la délibération que les tests avec des données du Registre national s'effectueront au profit d'instances habilitées qui disposent d'un accès au Registre national. Les finalités pour lesquelles des instances demandent un accès au Registre national sont toujours liées à leurs missions et/ou activités propres. Utiliser des données du Registre national pour de simples finalités de test n'est donc pas possible sur la base des autorisations habituelles. L'autorisation accordée le permet pour Fedict, le concepteur et celui qui propose les applications au profit d'instances habilitées.

28. Il s'agit donc bel et bien ici d'une finalité spécifique. Lorsqu'un citoyen vérifiera qui a consulté ses données, il apparaîtra donc clairement que ses données ont été utilisées pour des finalités de test. Fedict, en tant qu'instance autorisée concernée, devra, en cas d'interpellation, indiquer en vue de l'application de quelle instance habilitée le test a été effectué.

29. Le Service public fédéral Intérieur remet également en cause la proportionnalité de l'accès permanent octroyé. À l'époque, ce dossier a aussi été transmis au Service public fédéral Intérieur en vue de recueillir l'avis technique et juridique prescrit par l'article 31, § 3, premier alinéa de la LVP. Cet avis technique et juridique, reçu par le comité le 5 mai 2008, ne formulait toutefois aucune remarque concernant l'accès permanent envisagé.

30. La *ratio legis* de l'accès permanent octroyé est la suivante :

- les tests et l'entretien d'applications ne s'effectuent pas selon une périodicité déterminée mais en fonction des besoins et d'incidents éventuels ;
- on ne peut pas déterminer à l'avance quand Fedict a besoin de données de test.

31. Un accès permanent offre donc à Fedict la possibilité d'aller chercher des données test dans le Registre national lorsque cela est nécessaire pour la finalité définie dans la délibération RN n° 19/2008. Il serait peu pratique de souhaiter que Fedict demande un accès au cas par cas. Il s'agit donc d'un accès permanent qui n'a pas pour conséquence que le Registre national soit interrogé en permanence par Fedict.

32. Le Comité sectoriel du Registre national a évalué le délai de conservation sur la base du dossier introduit par Fedict. Dans son avis technique et juridique, le Service public fédéral Intérieur n'a émis aucune critique quant au délai de conservation proposé d'un an maximum.

33. Dans les délibérations du Comité sectoriel du Registre national, un délai de conservation maximal est régulièrement proposé. Cela a lieu dans des cas où, en fonction de la situation, les données peuvent être détruites plus tôt dans certains cas que dans d'autres. En pareil cas, il relève toujours de la responsabilité de l'instance habilitée de veiller à détruire les données dès qu'elles n'ont plus d'utilité, même avant l'expiration de ce délai. Si à l'occasion d'un contrôle, il s'avère que cela n'a pas été effectué, cette instance s'expose à des sanctions.

34. La Commission constate qu'un délai de conservation maximal n'a jamais conduit, dans une multitude d'autres dossiers, à une quelconque remarque à cet égard dans les avis techniques et juridiques émanant du Service public fédéral Intérieur.

35. Enfin, le Service public fédéral Intérieur attire l'attention sur le fait qu'un environnement de test est actuellement disponible auprès du Registre national. Le Comité sectoriel du Registre national a entre-temps interpellé Fedict et CORVE pour vérifier si cet environnement de test répond à leurs besoins. Si c'est le cas, ce comité entreprendra des actions appropriées. Quoi qu'il en soit, la discussion sur le test des données de production peut être solutionnée si les services du Registre national mettent à disposition un environnement d'acceptation représentatif performant – une copie avec les mêmes fonctionnalités que le Registre national proprement dit -, ce qui n'est pas le cas jusqu'à présent.

PAR CES MOTIFS,

la Commission estime que les remarques formulées par le Service public fédéral Intérieur concernant la délibération RN n° 19/2008 du 7 mai 2008 ne sont pas de nature à mettre en cause cette délibération.

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

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere