Avis n° 20/2014 du 19 mars 2014

Objet : demande d'avis concernant le projet d'arrêté royal *fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification pour applications publiques numériques qui utilisent des moyens d'identification sans fil* (CO-A-2014-015)

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 29 ;

Vu la demande d'avis de monsieur Hendrik Bogaert, Secrétaire d'État à la Fonction publique et à la Modernisation des Services publics, reçue le 11/02/2014 ;

Vu les informations complémentaires reçues le 27/02/2014 ;

Vu le rapport de Monsieur Frank Robben ;

Émet, le 19 mars 2014, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS

1. Par courrier du 7 février 2014, le Secrétaire d'État à la Fonction publique et à la Modernisation des Services publics (ci-après "le demandeur") a sollicité l'avis en extrême urgence de la Commission concernant le projet d'arrêté royal *fixant les conditions, la procédure et les conséquences de l'agrément de services d'identification pour applications publiques numériques qui utilisent des moyens d'identification sans fil* (ci-après "le projet d'AR").

2. La Commission émet dès lors ci-après un avis en extrême urgence concernant le projet d'AR, sur la base des informations dont elle dispose.

II. LE CADRE LÉGAL

3. Le projet d'AR exécute les articles 133 à 136 de la *loi-programme* du 8 avril 2003 qui prévoient un cadre légal pour l'offre de services électroniques aux citoyens via des portails ou des sites Internet, et ce par le biais d'une identification et d'une authentification électroniques du citoyen.

4. Le projet d'AR est également pris en exécution de la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral* qui reconnaît le service public fédéral Technologie de l'Information et de la Communication (Fedict) en tant qu'intégrateur de services pour l'administration fédérale. L'article 4, 3° de cette loi établit que Fedict doit promouvoir et veiller à l'homogénéité des droits d'accès aux banques de données. Selon l'article 4, 4° de cette loi, Fedict élabore les modalités techniques visant à développer les canaux d'accès de la manière la plus efficace et la plus sûre possible.

III. EXAMEN DE LA DEMANDE D'AVIS

A. Contexte de la demande

5. Conformément au rapport au Roi, le projet d'AR s'inscrit dans la politique d'e-gouvernement globale du gouvernement. L'utilisation croissante des tablettes et des smartphones confronte l'administration au défi d'également pouvoir offrir sur ces nouveaux appareils l'accès aux applications publiques numériques, toujours plus nombreuses. Simultanément, des solutions sont cherchées afin de simplifier, pour les utilisateurs, l'identification à l'aide de la carte d'identité électronique. Pour s'identifier à l'aide de la carte d'identité électronique, il est à l'heure actuelle généralement fait

usage d'un lecteur de cartes filaire. Cependant, de nombreux citoyens ne disposent pas d'un tel lecteur et son utilisation est vue par beaucoup comme un obstacle, en raison de l'obligation d'installer le logiciel requis.

6. Le projet d'AR entend dès lors créer un cadre dans lequel un fournisseur de services d'identification pour applications numériques non publiques qui utilisent un moyen d'identification sans fil pourra obtenir un agrément afin de pouvoir également mettre à disposition le moyen d'identification sans fil qu'il propose pour une utilisation dans des applications publiques numériques. À cet égard, il est par exemple possible d'envisager que les moyens d'identification sans fil des systèmes de banque à domicile soient aussi utilisés pour lire les cartes d'identité électroniques dans le cadre d'applications publiques numériques.

B. Point de vue général de la Commission

7. La Commission constate que le projet d'AR comporte plusieurs dispositions qui règlent déjà en détail les modalités d'identification et d'authentification des citoyens, en particulier dans l'annexe II *"Spécifications fonctionnelles et techniques du service d'identification".*

8. L'article 16 de la LVP prévoit qu'un responsable du traitement doit prendre les mesures techniques et organisationnelles requises. Ces mesures doivent assurer un niveau de protection adéquat. Afin de déterminer quel niveau de sécurité est adéquat ou approprié, la loi prévoit quatre critères : les possibilités ou l'état de la technique, les frais qu'entraîne l'application de ces mesures, la nature des données à protéger et les risques potentiels. Ces critères impliquent notamment que le responsable du traitement doit constamment s'informer des diverses techniques existant sur le marché afin de sécuriser les données et leur traitement. Il doit en effet vérifier si ce qui convenait auparavant convient toujours à présent[1].

9. Dans cette optique, la Commission plaide pour une approche qui permet d'adapter les mesures de sécurité (techniques) à tout moment et de manière flexible. Si celles-ci sont définies en détail dans la réglementation – comme proposé dans le projet d'AR –, chaque adaptation des mesures requerra nécessairement aussi une modification du projet d'AR, ce qui implique systématiquement une procédure longue et fastidieuse. Dans le cas présent, ce manque de flexibilité peut avoir pour effet que, dans la pratique, l'article 16 de la LVP demeure lettre morte car il y a un risque de ne pas pouvoir anticiper (suffisamment tôt) de nouvelles évolutions technologiques. Afin de limiter ce risque, la Commission recommande que le projet d'AR entre moins dans les détails et notamment qu'il prévoie simplement les fonctionnalités auxquelles le système visé devra

[1] D. De Bot, *Verwerking van persoonsgegevens*, Antwerpen, Kluwer, 2001, p. 253.

satisfaire. L'annexe II contenant les spécifications techniques et les mesures de sécurité concrètes ne doit dès lors pas être reprise dans le projet d'AR. Le projet d'AR doit par contre prévoir que la définition et la validation de ces spécifications et de ces mesures puisse être déléguée au Comité sectoriel compétent, à savoir le Comité sectoriel du Registre national. Fedict peut introduire un dossier à cet effet auprès de ce Comité. Cette méthode gagnerait en flexibilité et offrirait également dans ce cas davantage de garanties en matière de protection des données à caractère personnel.

C. Commentaire des articles

L'analyse qui suit concerne uniquement les articles du projet d'AR qui sont pertinents pour l'application de la LVP.

10. L'*article 1er* contient la liste des différentes définitions. La définition de "moyen d'identification sans fil" et de "moyen d'identification filaire" n'est pas tout à fait claire dans la version néerlandaise : la différence entre les deux se base-t-elle sur la présence ou l'absence d'un fil ? Selon les explications du demandeur, il s'agit en effet de lecteurs de cartes filaires et sans fil. Il est recommandé de clarifier cet aspect.

11. L'*article 5* prévoit que lors de la vérification de la carte d'identité électronique, le moyen d'identification sans fil utilise les opérations cryptographiques relatives au certificat d'identité de la carte d'identité électronique. À cet égard, le demandeur peut renvoyer aux dispositions légales pertinentes concernant la carte d'identité électronique. Le cas échéant, ces dispositions peuvent être reprises dans l'Annexe II du projet d'AR.

12. Conformément à l'*article 7*, l'utilisateur doit d'abord s'identifier auprès de l'administration fédérale pour sélectionner le service d'identification pour lequel il souhaite s'enregistrer. Il doit ensuite également s'enregistrer de façon unique auprès du prestataire de services. On ne sait pas clairement quelles données sont enregistrées auprès du prestataire de services. D'après les explications fournies par le demandeur, il s'agit des données nécessaires au contrôle du certificat d'identité : le numéro de série et l'émetteur du certificat d'identité. La Commission rappelle au demandeur que si des données à caractère personnel sont traitées par le prestataire de services, conformément à l'article 4, § 1, 3° de la LVP, ces données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

13. D'après l'*article 8*, l'enregistrement de l'utilisateur n'est possible que si, au moment de l'enregistrement, le certificat d'identification de la carte d'identité électronique n'est pas échu, n'est pas révoqué et s'il est émis par une autorité de certification agréée et non révoquée. Ces conditions

sont réellement nécessaires pour garantir la sécurité du service conformément à l'article 16 de la LVP - par exemple en cas de vol d'une carte d'identité et du code PIN y afférent, où Docstop a été prévenu - et il convient de veiller à ce que ces conditions soient scrupuleusement respectées par le prestataire de services.

14. L'*article 11* dispose que lors de chaque identification, le service d'identification envoie à l'autorité d'agrément le code d'identification unique de l'utilisateur, sur la base duquel l'autorité d'agrément détermine l'identité de l'utilisateur. On ne sait pas clairement de quelles données se compose ce code d'identification unique. Il convient en outre de faire remarquer que si ce code d'identification unique utilise le numéro d'identification du Registre national, pour cette utilisation, le prestataire de services doit ou devra être autorisé par le Comité sectoriel du Registre national. D'après les informations fournies par le demandeur, il s'agirait d'un code d'identification aléatoire.

15. En vertu de l'*article 12*, le prestataire de services garantit que l'utilisation du moyen d'identification sans fil n'est possible que si, au moment de l'enregistrement, le certificat d'identification de la carte d'identité électronique n'est pas échu, n'est pas révoqué et s'il est émis par une autorité de certification agréée et non révoquée. Comme déjà indiqué au point 13, il s'agit d'une condition cruciale pour la sécurité du service presté, conformément à l'article 16 de la LVP. Le prestataire de services doit dès lors pouvoir disposer immédiatement de toutes les informations pertinentes, par exemple de celles émanant de Docstop.

16. D'après l'*article 15, § 1er,* le prestataire de services ne prend pas connaissance des applications publiques numériques auxquelles l'utilisateur demande l'accès à l'aide de son service d'identification. Ceci est répété à l'article 22 de l'Annexe II du projet d'AR. Il s'agit d'une disposition importante dans le projet d'AR, qui constitue également une application de l'article 4, § 1, 3° de la LVP. Il importe que le prestataire de services n'ait pas connaissance de l'application d'e-gouvernement consultée par l'utilisateur. Les finalités visées dans le projet d'AR ne nécessitent en effet pas que le prestataire de services dispose de cette information. Cela pourrait en outre constituer, dans le chef du prestataire de services, un traitement de données sensibles (par exemple une consultation de la plate-forme eHealth) conformément à la LVP, lequel fait l'objet de dispositions particulières.

17. L'*article 15, § 2* prévoit que le prestataire de services établit une piste d'audit sécurisée afin que les données puissent être reconstituées pour chaque transaction spécifique, et ce en vue de la sécurisation des données et de la protection de la vie privée. À cet effet, le prestataire de services conserve pour une durée de dix ans l'identité de l'utilisateur, le service d'identification avec lequel l'utilisateur s'identifie et le moment de l'identification. On ne sait pas clairement ce qu'il y a lieu d'entendre par "identité de l'utilisateur". Cela implique-t-il également un traitement du numéro

d'identification du Registre national ? Cet aspect doit être clarifié et le principe de proportionnalité doit être respecté, conformément à l'article 4, § 1, 3° de la LVP. D'après les informations fournies par le demandeur, il s'agirait uniquement du nom de l'utilisateur, ce qui peut être considéré comme étant proportionnel. Le choix d'un délai de conservation de 10 ans, qui pourrait être dicté par certains délais de prescription en matière pénale, mérite aussi d'être expliqué dans le rapport au Roi.

18. À l'*article 5 de l'Annexe II* du projet d'AR, au point 2, on mentionne les "informations minimales" qui doivent être enregistrées par le prestataire de services afin de confirmer la validité de la carte d'identité électronique au moment de l'identification. D'après les informations fournies par le demandeur, il s'agit des données nécessaires pour pouvoir procéder à un contrôle du certificat d'identité : le numéro de série et l'émetteur du certificat d'identité.

19. À l'*article 6 de l'Annexe II* du projet d'AR, il est question d'un code d'identification unique. À cet égard, la Commission renvoie également à la remarque qu'elle a formulée au point 14.

PAR CES MOTIFS,

la Commission émet un avis **favorable** sur le contenu actuel du projet d'AR, à condition qu'il soit tenu compte des remarques formulées aux points 9, 14, 16-17 du présent avis.

L'Administrateur f.f., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere