Avis n° 48/2016 du 21 septembre 2016

Objet : avis concernant l'avant-projet de loi relative à l'identification électronique (CO-A-2016-032)

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 Jan DEPREST, Président du Service public fédéral ICT, reçue le 13/05/2016 ;

Vu les textes adaptés de l'avant-projet, reçus le 25/05/2016, le 13/07/2016 et le 14/09/2016, et vu les explications complémentaires reçues le 22/08/2016 ;

Vu le rapport de Monsieur Ivan VANDERMEERSCH ;

Émet, le 21 septembre 2016, l'avis suivant :

REMARQUE PRÉALABLE

La Commission attire l'attention sur le fait qu'une nouvelle réglementation européenne relative à la protection des données à caractère personnel a été promulguée récemment : le Règlement général relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et la Directive Police et Justice. Ces textes ont été publiés au journal officiel de l'Union européenne le 4 mai 2016[1].

Le Règlement, couramment appelé GDPR (General Data Protection Regulation), est entré en vigueur vingt jours après sa publication, soit le 24 mai 2016, et est automatiquement applicable deux ans plus tard, soit le 25 mai 2018. La Directive Police et Justice doit être transposée dans la législation nationale au plus tard le 6 mai 2018.

Pour le Règlement, cela signifie que depuis le 24 mai 2016, pendant le délai d'exécution de deux ans, les États membres ont d'une part une obligation positive de prendre toutes les dispositions d'exécution nécessaires, et d'autre part aussi une obligation négative, appelée "devoir d'abstention". Cette dernière obligation implique l'interdiction de promulguer une législation nationale qui compromettrait gravement le résultat visé par le Règlement. Des principes similaires s'appliquent également pour la Directive.

Il est dès lors recommandé d'anticiper éventuellement dès à présent ces textes. Et c'est en premier lieu au(x) demandeur(s) de l'avis qu'il incombe d'en tenir compte dans ses (leurs) propositions ou projets. Dans le présent avis, la Commission a d'ores et déjà veillé, dans la mesure du possible et sous réserve d'éventuels points de vue complémentaires ultérieurs, au respect de l'obligation négative précitée.

I. CONTEXTE

1. L'avant-projet de loi relative à l'identification électronique, ci-après "l'avant-projet", comprend 2 volets. Le premier volet comporte un certain nombre de mesures qui sont nécessaires pour appliquer

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (règlement général sur la protection des données)
Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision-cadre 2008/977/JAI du Conseil*
http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC
)

le chapitre II du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 *sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE* (ci-après "le règlement 910/2014").

2. Le deuxième volet étaie juridiquement l'identification électronique pour les applications publiques en ce qui concerne la Belgique.

3. L'identification électronique se fait via des systèmes numériques et va de pair avec le traitement automatisé de données à caractère personnel. Les dispositions de la LVP sont donc applicables. L'analyse se limite aux articles qui donnent lieu au traitement de données à caractère personnel.

II. EXAMEN QUANT AU FOND

A. APPLICATION DU CHAPITRE II DU RÈGLEMENT 910/2014

Généralités

4. Afin de pouvoir utiliser des services électroniques, une identification et une authentification électroniques sont généralement requises. Celles-ci constituent une pierre d'achoppement pour l'utilisation transfrontalière de services électroniques car un citoyen ne peut pas utiliser son moyen d'identification électronique (ci-après MIE) parce que son système national d'identification et d'authentification électroniques n'est pas reconnu dans les autres États membres.
Le règlement 910/2014 entend lever cet obstacle, en tout cas en ce qui concerne l'identification et l'authentification vis-à-vis du secteur public. Le chapitre II définit la manière dont cela s'effectuera, à savoir en élaborant un système de reconnaissance mutuelle obligatoire de MIE[1]. Les MIE étrangers ainsi reconnus doivent pouvoir être utilisés en Belgique sans entraves. Des règlements d'exécution établissent des règles plus détaillées en vue de la mise en application de ce système de reconnaissance mutuelle. À titre d'exemple :

a) Le règlement d'exécution (UE) n° 2015/1501 traite de ce qu'on appelle le "cadre d'interopérabilité" (qui a pour but d'assurer l'interopérabilité des schémas d'identification électronique notifiés par les États membres à la Commission européenne). Ce règlement

[1] L'article 7 du règlement 910/2014 contient les conditions qu'un schéma d'identification électronique doit remplir pour être éligible pour la notification à la Commission européenne. Au plus tard un an après la publication par la Commission européenne des schémas d'identification électronique qui ont été notifiés, ceux-ci doivent être reconnus (articles 6.1 et 9.2 du règlement 910/2014).

d'exécution définit également des règles relatives à la sécurité des données et, dans ce cadre, fait reposer une importante responsabilité auprès des dits "nœuds"[2].

b) Le règlement d'exécution (UE) n° 2015/1502 fixe des spécifications techniques, des normes et des procédures minimales permettant de définir le niveau de garantie d'un MIE. Ce règlement d'exécution contient également des règles en matière de "demande et enregistrement", de "preuve et vérification d'identité", de "délivrance et activation".

5. La Commission constate en outre que dans le cadre d'une identification et d'une authentification transfrontalières, ce n'est pas le numéro de Registre national qui est communiqué mais le STORK-ID (constitué sur la base du numéro de Registre national). Selon les informations complémentaires de l'auteur de l'avant-projet, reçues par la Commission le 22 août 2016, la Belgique n'est pas un cas isolé à ce niveau et chaque pays européen travaille avec un numéro transnational unique afin d'identifier ses citoyens dans un contexte transnational[3]. Afin d'expliquer la distinction entre l'utilisation d'un numéro unique dans l'identification transfrontalière et l'identification nationale, il serait préférable d'intégrer dans l'exposé des motifs les informations complémentaires que l'auteur de l'avant-projet a transmises à cet égard à la Commission le 22 août 2016.

Article 5, § 1er de l'avant-projet

6. En fait, il s'agit d'une intervention de légistique purement formelle qui met en conformité avec le règlement 910/2014 toute réglementation belge prescrivant l'utilisation de MIE belges pour accéder à un service électronique, sans que des dispositions individuelles de la réglementation belge ne doivent être adaptées. En vertu de cette disposition, les MIE étrangers reconnus présentant le même niveau de garantie que le MIE belge devront être autorisés.

7. Vu les dispositions du règlement 910/2014 d'une part et le fait que l'équivalence se limite aux MIE présentant le même niveau de garantie que celui requis par la réglementation belge d'autre part, cela ne pose pas de problèmes spécifiques du point de vue de la LVP. Par pur souci d'exhaustivité, la Commission attire l'attention sur le fait qu'il faut veiller à ce que la sécurité de la chaîne par le biais de laquelle le processus d'identification et d'authentification se déroule à l'aide du MIE étranger soit assurée et à ce qu'une piste d'audit complète soit disponible. Cela requiert que tous les maillons de la

[2] En Belgique, Fedict assume le rôle de "nœud" (article 10 de l'avant-projet).

[3] À la question de savoir si un tel système dans notre pays ne conduit pas à un traitement inégal car les Belges sont obligés "en interne" de fournir leur numéro de Registre national alors que ce n'est pas le cas lors d'une identification transfrontalière, l'auteur répond ce qui suit : "*Toute personne reprise dans le Registre national est identifiée de manière unique par les instances belges habilitées à l'aide du numéro de Registre national. Ces mêmes personnes sont identifiées dans un contexte transnational européen à l'aide d'un numéro dérivé. Il s'agit donc des mêmes personnes qui sont identifiées d'une autre manière dans un autre contexte. (…) Cette méthode s'applique à toute personne de la même façon (en Belgique, le numéro de Registre national, en dehors de la Belgique et au sein de l'UE, d'une autre manière (…)*" [traduction libre réalisée par le Secrétariat de la Commission, en l'absence de traduction officielle].

chaîne puissent être identifiés et que des accords et/ou des garanties entre tous les maillons de la chaîne soient convenu(e)s (circles of trust ou cercles de confiance).

Article 5, § 2 de l'avant-projet

8. Le considérant 17 - qui se rapporte à l'article 7, f), deuxième alinéa du règlement 910/2014 - incite les États membres à encourager le secteur privé à utiliser des MIE notifiés.

9. L'article 5, § 2 de l'avant-projet recourt à la possibilité offerte par l'article 7, f), deuxième alinéa du règlement 910/2014, à savoir soumettre l'utilisation par le secteur privé de MIE notifiés à des conditions. Le Roi est chargé de définir ces conditions.

10. Actuellement, il est impossible à la Commission d'évaluer l'impact que cela aura au niveau du traitement de données à caractère personnel. Il serait dès lors préférable de recueillir préalablement l'avis de la Commission concernant cet arrêté royal.

11. L'article 11.1 du Règlement d'exécution (UE) 2015/1501 de la Commission européenne du 8 septembre 2015[4] dispose que dans le cadre d'une transaction **transfrontalière**, un ensemble minimal de données d'identification personnelle - énumérées dans l'annexe - doit être transmis. Cet ensemble comporte **obligatoirement** : le(s) nom(s) de famille actuel(s), le(s) prénom(s) actuel(s), la date de naissance et l'identifiant unique créé par l'État membre expéditeur conformément aux spécifications techniques aux fins de l'identification transfrontalière et qui soit aussi persistant que possible dans le temps. Les données suivantes sont **optionnelles** : prénom(s) et nom(s) de famille à la naissance, lieu de naissance, adresse actuelle et sexe.

12. La formulation de ce règlement d'exécution ne fait pas de distinction entre une authentification transfrontalière au profit d'un service public et celle au profit du secteur privé.

13. La question se pose de savoir si en application de l'article 7, f), deuxième alinéa du règlement 910/2014, le Roi peut poser comme condition qu'un ensemble plus limité de données d'identification personnelle soit transmis lorsque l'authentification se fait à l'aide du MIE au profit d'un acteur du secteur privé.

14. Si tel n'est pas le cas, cela signifie concrètement que des informations du Registre national sont fournies (voir l'article 7 de l'avant-projet) à des entreprises commerciales étrangères. En vertu

[4] Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 *sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur*, adopté en exécution des articles 9 et 12 du règlement 910/2014.

de l'actuelle loi du 8 août 1983 *organisant un registre national des personnes physiques*, les entreprises commerciales – qu'il s'agisse d'entreprises étrangères ou belges – n'entrent pas en ligne de compte pour obtenir des informations du Registre national ou utiliser le numéro de Registre national.

15. La Commission profite de l'occasion pour attirer l'attention sur la problématique des données qui peuvent être transmises de manière optionnelle. Avant que celles-ci soient transférées, il faudra préalablement contrôler si leur envoi est proportionnel à la lumière de la finalité poursuivie et si oui, quelles données parmi celles-ci sont proportionnelles (article 4, § 1, 3° de la LVP). Il ressort de l'article 7 de l'avant-projet que le Service public fédéral Technologie de l'Information et de la Communication (ci-après Fedict) se chargera de l'envoi. Dès lors, c'est Fedict qui doit veiller au respect du principe de proportionnalité. La Commission estime qu'il n'appartient pas à Fedict, en tant que nœud technique, de déterminer quelles données optionnelles sont proportionnelles dans un cas concret. La Commission ou le comité sectoriel compétent sont mieux placés pour en décider et il serait dès lors souhaitable de reprendre cette information dans la réglementation. Il est quoi qu'il en soit recommandé d'informer la personne concernée avant de procéder à l'envoi effectif de données optionnelles de manière à ce qu'elle ait la possibilité de mettre un terme à l'opération lorsqu'elle juge que la communication d'une ou de plusieurs données optionnelles n'est pas pertinente.

Article 6, § 1er de l'avant-projet

16. Il ressort de l'article 6.1. du règlement 910/2014 que la reconnaissance mutuelle obligatoire ne joue que pour les MIE dont le niveau de garantie est égal ou supérieur à celui requis par l'organisme du secteur public concerné et pour autant que ce niveau soit substantiel ou élevé. En cas de niveau de garantie "faible", la reconnaissance est facultative (article 6.2. du règlement 910/2014).

17. C'est à cette fin que l'article 6, § 1er de l'avant-projet oblige les autorités qui proposent des services en ligne à déterminer le niveau de garantie nécessaire, requis pour accéder à ces services. C'est essentiel pour pouvoir établir si la reconnaissance mutuelle de MIE est d'application et, dans l'affirmative, à l'aide de quel MIE un accès doit être accordé.

18. L'autorité (= le responsable du traitement) qui propose un service en ligne est la mieux placée pour évaluer le niveau de garantie requis. Elle devra réaliser une analyse approfondie qui tiendra notamment compte de la quantité de données qui sont collectées par personne, du nombre de personnes dont des données sont collectées, de la nature des données qui sont collectées (sensibles ou pas), du risque d'accès aux données, du risque de modification/de destruction des données par des personnes non habilitées et des dommages que cela peut engendrer, du fait que seuls des droits de lecture sont accordés ou également des droits d'écriture, du fait que des tiers peuvent obtenir un accès/effectuer des opérations au profit d'un tiers, ...

Article 6, § 2 de l'avant-projet

19. La définition du niveau de garantie des MIE[5] qui seront notifiés par Fedict est une décision lourde de conséquences pour tous les services publics qui mettent à disposition des services électroniques. Lorsque le niveau de garantie d'un MIE est défini comme "substantial" ou "high" et donc notifié comme tel, les services publics belges qui accordent un accès sur la base d'un MIE présentant un tel niveau seront obligés d'autoriser les MIE étrangers notifiés du même niveau, ce qui peut occasionner des problèmes.

20. Afin d'éviter que des autorités belges ne soient mises devant le fait accompli, l'obligation, dans le chef de Fedict, de consulter le plus grand nombre possible d'acteurs concernés, via le Collège des présidents des services publics fédéraux et des services publics de programmation, le Collège des administrateurs délégués des institutions de la sécurité sociale et le Collège des administrateurs délégués des organismes d'intérêt public fédéraux, avant la définition du niveau de garantie et la notification, est une bonne chose. Cela permet à Fedict, avant de procéder à la notification, de réaliser une pondération réfléchie qui tient compte aussi bien des aspects techniques que pratiques.

Article 7 de l'avant-projet

21. Le paragraphe 1er de cet article charge Fedict, lors d'une identification transfrontalière, de fournir les données d'identification personnelle obligatoires et optionnelles telles que définies dans le règlement d'exécution (UE) 2015/1501. À cet effet, les §§ 2 et 3 de l'article 7 de l'avant-projet accordent à Fedict un accès aux informations du Registre national.

22. Il est donc dérogé à la compétence de principe du Comité sectoriel du Registre national telle que prévue par la loi du 8 août 1983. Le législateur peut, via une norme juridique de rang égal, prévoir des exceptions à la procédure imposée par la loi du 8 août 1983[6].

23. Les données d'identification qui doivent obligatoirement être envoyées sont reprises sur la puce de la carte d'identité électronique (eID). En théorie, ces données pourraient être lues et ensuite transmises. Ce n'est toutefois pas une option étant donné le fait que :

- selon toute probabilité, d'autres MIE que l'eID seront également notifiés ;

---

[5] Le règlement d'exécution (UE) n° 2015/1502 fixe des spécifications techniques, des normes et des procédures minimales permettant de définir le niveau de garantie.

[6] Concernant cette problématique, voir également les points 22 et 23 de l'avis de la Commission n° 15/2006 du 14 juin 2006 *relatif au projet d'arrêté royal réglant la collaboration à l'association chargée de l'enregistrement du kilométrage des véhicules.*

- l'eID sera également utilisée d'une manière non-connectée, rendant la lecture de la puce impossible.

24. La manière la plus pratique de transmettre ces données est donc de recourir à la source authentique pertinente, à savoir le Registre national. Fedict extraira juste les données obligatoires du Registre national. Il ne les extrait pas pour son propre usage mais pour une communication à des instances publiques et/ou privées étrangères. On pourrait affirmer qu'une communication impropre d'informations du Registre national est organisée au profit d'instances qui, sur la base de la loi du 8 août 1983, n'entrent pas en ligne de compte pour obtenir une telle communication. À la lumière de cet élément, la Commission estime qu'il convient de régir la communication des données du Registre national à des acteurs étrangers afin d'éviter toute discussion.

25. En ce qui concerne les données d'identification qu'il faut obligatoirement fournir, vu ce que prévoit le règlement d'exécution (UE) 2015/1501, aucun problème ne se pose en matière de finalité et de proportionnalité. Quant aux données d'identification qui peuvent être communiquées de manière optionnelle, la situation est quelque peu différente. Il faudra évaluer au cas par cas si la communication des données optionnelles est proportionnelle, compte tenu de la finalité. Dans ce cas, l'avis du comité sectoriel compétent ou de l'autorité de contrôle devra être préalablement recueilli. En vertu du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, la Commission et ses comités sectoriels peuvent faire l'objet d'une réforme. La formulation proposée devrait garantir un contrôle indépendant de la proportionnalité, quel que soit le résultat de cette réforme. À cet égard, la Commission renvoie à sa remarque émise au point 15.

26. Ce que l'on peut attendre de Fedict en vue de la transparence, c'est qu'avant de lancer la procédure d'identification et d'authentification, il signale à la personne concernée quelles données d'identification minimales doivent être envoyées en vertu de l'obligation imposée par le règlement d'exécution (UE) 2015/1501 et que ces données seront à cet effet extraites du Registre national. La personne concernée qui ne souhaite pas que cette communication ait lieu doit ensuite avoir la possibilité de ne pas lancer la procédure.

27. Étant donné que ce paragraphe constitue une exception aux dispositions de la loi du 8 août 1983, il est recommandé d'utiliser la même terminologie que dans cette loi et de remplacer le passage :

> *"(…) le service public fédéral Technologie de l'Information et de la Communication a le droit d'obtenir les données nécessaires du Registre national"*

par :

> *"(...) le service public fédéral Technologie de l'Information et de la Communication est autorisé à collecter les données visées au § 1er dans le Registre national".*

28. En remplaçant "*les données nécessaires*" par "*les données visées au § 1er*", on insiste sur le fait que l'accès est limité aux données qui font partie de l'ensemble minimal de données tel que défini dans l'annexe du règlement d'exécution (UE) 2015/1501.

29. Le paragraphe 3 anticipe une éventuelle extension future des données optionnelles qui deviendrait possible en vertu du règlement 910/2014 ou de son règlement d'exécution en prévoyant déjà à cet effet par le biais de la présente loi un accès au Registre national. Tout comme c'était le cas pour le paragraphe 2, il est préférable d'harmoniser la formulation avec la terminologie utilisée dans la loi du 8 août 1983. Il est dès lors proposé de remplacer le texte de ce paragraphe comme suit :

> *"Pour satisfaire à une obligation du règlement 910/2014 ou à l'un de ses actes d'exécution qui permet l'échange de données d'identification personnelle supplémentaires, le service public fédéral Technologie de l'Information et de la Communication est autorisé à collecter les données correspondantes dans le Registre national, après avis du comité sectoriel compétent ou de l'autorité de contrôle telle que visée au chapitre VI du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE."*

Article 8 de l'avant-projet

30. Cet article organise la surveillance et le contrôle des schémas d'identification électronique notifiés.

31. La Commission constate tout d'abord que l'avant-projet n'indique pas quelle instance assurera le rôle d'organe de contrôle. À cet égard, l'auteur de l'avant-projet a précisé ce qui suit dans ses explications complémentaires du 22/08/2016 : "*Nous sommes conscients du fait que cette compétence doit être attribuée au plus vite à un organe neutre doté de l'expertise nécessaire et nous en ferons dès lors une priorité.*" [traduction libre réalisée par le Secrétariat de la Commission, en l'absence de traduction officielle]. La Commission adhère à ce point de vue et estime qu'il est préférable de régler la désignation de cet organe dans l'avant-projet. Dans la mesure où Fedict est coresponsable d'un MIE, à savoir l'eID, il ne semble pas indiqué qu'il assume le rôle d'organe de contrôle.

32. L'article 10 du règlement 910/2014 dispose qu'en cas d'altération partielle du schéma d'identification ou d'authentification électronique, l'État membre notifiant doit suspendre ou révoquer immédiatement l'identification et en informer la Commission européenne et les autres États membres. L'article 8, § 5 de l'avant-projet prévoit que l'organe de contrôle peut révoquer ou suspendre un schéma d'identification électronique notifié en cas d'altération de celui-ci. On ne sait pas clairement qui se chargera de la notification à la Commission européenne et aux autres États membres. Afin d'éviter tout malentendu, il faut préciser qui effectuera cette notification, vu l'importance de celle-ci et les éventuelles conséquences négatives au niveau du traitement des données si cette notification n'a pas lieu.

33. Les §§ 3 et 4 de l'article 8 de l'avant-projet régissent la situation dans laquelle l'organe de contrôle constate que l'émetteur d'un MIE ou la partie qui exécute la procédure d'authentification ne respecte pas les exigences du règlement 910/2014. Il s'agit donc manifestement de violations qui n'ont pas directement un impact sur l'intégrité du processus. Dans la mesure où cela signifie qu'il n'y a pas de risque que les données à caractère personnel traitées dans le cadre du processus soient compromises (perte, modification non autorisée, accès non autorisé, vol), il n'est pas problématique que l'instance concernée ait le temps de se conformer à nouveau aux exigences du règlement 910/2014. La Commission estime que dès le moment où la violation compromet les données à caractère personnel traitées, il faut prévoir la possibilité de suspendre ou de révoquer le schéma immédiatement, en attendant que l'instance concernée se mette en règle. À la lumière de l'article 16 de la LVP, on peut difficilement justifier que l'on laisse fonctionner un système qui ne remplit plus les exigences posées.

B. IDENTIFICATION ÉLECTRONIQUE POUR APPLICATIONS PUBLIQUES BELGES

Article 11, § 3 de l'avant-projet

34. Ce paragraphe déroge à nouveau à la compétence du Comité sectoriel du Registre national telle que régie par la loi du 8 août 1983. Une autorisation légale est accordée à Fedict pour utiliser le numéro de Registre national. Toutefois, la nécessité de cette exception légale n'est pas motivée. L'exposé des motifs relatif à cette disposition mentionne d'ailleurs que Fedict a déjà été autorisé par le Comité sectoriel du Registre national à utiliser le numéro de Registre national à des fins d'authentification. Ce paragraphe est donc superflu et doit être supprimé.

Article 12 de l'avant-projet

35. Cet article offre la possibilité d'accéder à des applications publiques numériques sur la base d'un service d'identification électronique, fourni par des acteurs qui ne sont pas des instances publiques. La Commission n'a aucune objection à ce principe en soi[7]. Quant au fond, la Commission ne peut actuellement pas se prononcer étant donné que la procédure, les conditions et les conséquences de l'agrément sont déterminées par le Roi. Il est prévu que l'avis du comité sectoriel compétent ou de l'autorité de contrôle soit demandé concernant l'arrêté royal qui doit être pris. En la matière, il est recommandé que l'avis de l'autorité de contrôle, normalement la Commission donc, soit recueilli plutôt que celui d'un comité sectoriel. Il est positif que, par analogie avec l'article 6, § 2 de l'avant-projet, une consultation préalable des acteurs concernés soit imposée (voir également le point 21).

36. Bien que le § 2 de l'article 12 de l'avant-projet charge le Roi de déterminer la procédure, les conditions et les conséquences relatives à l'agrément, certains aspects sont régis de manière univoque au § 5 de l'article 12. Tout d'abord, il est explicitement précisé que le fournisseur d'un service d'identification électronique agréé est autorisé par la loi à utiliser le numéro de Registre national. Il ressort de l'exposé des motifs que cette utilisation est limitée à la gestion des utilisateurs et des accès via le Federal Authentication Service (FAS, Service fédéral d'authentification) pour les services publics. En outre, l'exposé des motifs signale que si un fournisseur agréé souhaite utiliser le numéro de Registre national en dehors du cadre pour lequel il a été agréé, il devra à cet effet demander une autorisation auprès du comité sectoriel compétent. Par souci de clarté et afin d'éviter les malentendus, il conviendrait de reprendre cette limitation de l'utilisation du numéro de Registre national dans la loi.

37. Les fournisseurs agréés proposent généralement encore d'autres services, rendant réel le risque qu'ils utilisent les données à caractère personnel collectées pour la finalité pour laquelle ils ont été agréés à d'autres fins commerciales. Dans le commentaire des articles, il est précisé que des garanties seront demandées afin d'empêcher cela. Celles-ci feront partie des conditions d'agrément qui doivent être définies par le Roi. La Commission en prend acte et part du principe que le futur arrêté d'exécution susmentionné lui sera encore soumis ultérieurement pour avis. Parallèlement, elle insiste pour que soit déjà repris dans l'avant-projet le principe selon lequel les données à caractère personnel qui sont collectées dans le cadre de l'identification électronique ne peuvent pas être utilisées pour d'autres finalités.

[7] Dans le même sens : la Commission a émis un avis favorable dans son avis n° 20/2014 du 19 mars 2014 *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* qui rend possible le recours à des services de notification du secteur privé.

38. Le § 5 de l'article 12 de l'avant-projet accorde en outre aux services agréés d'identification électronique une autorisation légale d'utiliser le numéro de Registre national. Toutefois, la nécessité de cette exception légale au règlement repris dans la loi du 8 août 1983 n'est pas motivée. L'article lui-même dispose que le fournisseur d'un service agréé d'identification électronique doit être considéré comme un sous-traitant de l'autorité d'agrément, en l'occurrence Fedict, au sens de l'article 5, premier alinéa, 3° de la loi du 8 août 1983. Cette spécification suffit pour autoriser un tel fournisseur agréé sur la base des dispositions de la loi du 8 août 1983. Il n'y a dès lors aucune raison objective de reprendre une exception à la loi du 8 août 1983 pour ce groupe cible. Il est donc préférable que le texte de ce paragraphe se limite à :

> *"Le fournisseur d'un service agréé d'identification électronique est, pour l'application du présent article, considéré comme un sous-traitant de l'autorité d'agrément au sens de l'article 5, premier alinéa, 3° de la loi du 8 août 1983 organisant un registre national des personnes physiques."*

Par souci d'exhaustivité, la Commission attire l'attention sur le fait que si un fournisseur d'un service agréé d'identification électronique souhaite vérifier des données dans le Registre national en vue de ce service, il devra à cet effet demander une autorisation auprès du comité sectoriel compétent.

Article 13 de l'avant-projet

39. Le premier alinéa de cet article charge le titulaire du MIE d'en prendre soin (contrôle exclusif, protection contre la perte, le vol). Il est précisé dans le commentaire des articles que le contrôle exclusif implique notamment que les mots de passe doivent être tenus strictement confidentiels. La Commission constate que pour un certain nombre de citoyens, il est impossible par exemple de tenir leurs mots de passe strictement confidentiels.

40. De plus en plus de services sont exclusivement accessibles par voie numérique, alors qu'une partie de la population n'a pas pu s'y adapter. Lorsqu'une telle personne souhaite recourir à certains services, elle n'a souvent pas d'autre choix que de remettre par exemple son eID à un tiers et de lui fournir également son code PIN. Le tiers auquel elle a recours sera peut-être une personne qu'elle juge intègre et qui n'abusera donc pas de cet instrument. Qu'en est-il si ce tiers en abuse quand même ? Le titulaire du MIE a-t-il alors été négligent au sens de cet article de l'avant-projet ?

41. Le deuxième alinéa de l'article 13 de l'avant-projet dispose qu'un MIE qui n'est plus valable ou est révoqué ne peut plus être utilisé par le titulaire. Il ressort des explications complémentaires de l'auteur de l'avant-projet du 22 août 2016 qu'il n'est pas inhabituel de responsabiliser le titulaire d'un MIE de cette manière. Le texte révèle que seul le titulaire qui est de mauvaise foi (qui utilise son MIE

tout en sachant que ce dernier est expiré ou révoqué) est visé. La Commission en prend acte et pour être complète, attire l'attention sur le fait qu'une telle responsabilisation du titulaire ne porte évidemment pas préjudice aux obligations et aux responsabilités des autres acteurs (comme le fournisseur du MIE).

PAR CES MOTIFS,
la Commission

émet un avis favorable à condition qu'il soit tenu compte des remarques formulées aux points 5, 13-15, 25-29, 31, 32, 34, 36-38 et 41.

L'Administrateur f.f., Le Président,

(sé) An Machtens (sé) Willem Debeuckelaere