Avis n° 41/2008 du 17 décembre 2008

Objet : Demande d'avis concernant l'avant-projet de loi relative à l'institution et à l'organisation d'un Intégrateur de Services fédéral *(A/08/041)*

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 du Président du Comité de direction du Service fédéral public technologie de l'Information et de la Communication, M. DEPREST, reçue le 24/10/2008 ;

Vu le rapport de Madame Françoise D'HAUTCOURT ;

Émet le 17/12/2008 l'avis suivant :

I. OBJET DE LA DEMANDE

1. Aussi bien les citoyens que les entreprises attendent de plus en plus des autorités un service électronique sûr, intégré et personnalisé qui ne mette pas en péril la protection de leur vie privée.

2. Dixit l'Exposé des motifs – c'est possible à condition qu'une série de conditions essentielles soient remplies, à savoir :

- que des chaînes de processus optimisées soient adaptées à la logique des utilisateurs ainsi qu'à la répartition des missions entre les niveaux et services de l'Administration ;
- qu'une attribution automatique des droits et avantages soit proposée ;
- que des voies d'accès électroniques soient intégrées et personnalisées ;
- qu'une collecte unique et la réutilisation des informations factuelles soient prévues ;
- que les plates-formes de collaboration électronique soient interopérables et performantes ;
- que l'architecture TIC soit orientée vers les services ;

3. En instituant un Intégrateur de Services fédéral, rôle qui sera assumé par le Fedict, cet avant-projet veut créer un acteur fédéral qui sera investi d'un rôle de coordination et de pilotage en la matière. En ce qui concerne le secteur qui ressortit à sa compétence, il fera également office de point de contact central en vue de la concertation avec les autres niveaux des pouvoirs publics.

4. Les points d'attention de cet avant-projet sont :

- la protection des données ;
- la sécurité de l'information ;
- le pilotage de l'Intégrateur de Services fédéral ;
- la concertation entre les différents intégrateurs de services et la délimitation de leur terrain d'action ;
- le contrôle.

II. EXAMEN DU TEXTE DU PROJET

A. CONTEXTE

5. Il n'est pas pensable qu'un service ou un pouvoir public seul ne puisse développer un service électronique sûr, intégré et personnalisé. Il existe, en effet, trop de synergies entre les divers services et niveaux des pouvoirs publics. Sans concertation et sans accords sérieux, l'e-government

n'est pas possible. Les divers services publics en sont d'ailleurs conscients. Il suffit pour s'en convaincre de se référer à l'Accord de coopération du 28 septembre 2006 *entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire française et la Commission communautaire commune concernant les principes pour un e-gouvernement intégré et la construction, l'utilisation et la gestion de développements et de services d'un e-gouvernement intégré*[1], qui souligne la nécessité d'une approche commune. L'article 7 de cet accord souligne par ailleurs que la protection de la vie privée doit toujours faire l'objet d'une attention particulière.

6. Cela indique une volonté d'interopérabilité[2] au sein – avant tout – du contexte belge. Suite à la décision 2004/387/CE du Parlement européen et du Conseil du 21 avril 2004 *relative à la fourniture interopérable de services paneuropéens d'administration en ligne aux administrations publiques, aux entreprises et aux citoyens*, cette interopérabilité prendra forcément à terme une dimension européenne.

7. L'article 2 de cet accord de coopération énumère les principes que tous les niveaux administratifs estiment devoir être respectés dans le développement de leurs initiatives et projet d'e-government. Ces principes sont les mêmes que les conditions essentielles reprises dans l'Exposé des motifs. L'avant-projet s'inscrit donc dans le prolongement de cet accord de coopération en ce sens qu'il procure au niveau fédéral un cadre réglementaire dans lequel élaborer des projets d'e-government intégrés, respectueux des droits des citoyens.

8. Il est en effet exact que dans sa délibération AF n° 05/2007 du 21 mars 2007 la Commission écrivait :

> *La Commission s'attend à ce que les banques de données relevant de la compétence du Comité sectoriel pour l'Autorité fédérale soient de plus en plus consultées à l'avenir.*
>
> *Il est plus que probable que l'on ne visera pas toujours simplement un accès à une banque de données ou la communication de données d'une telle banque de données. Dans un certain nombre de cas, des liens entre ces banques de données et d'autres fichiers de*

---

[1] Cet accord de coopération poursuit la coopération déjà échafaudée par l'Accord de coopération du 23 mars 2001 *entre l'État fédéral, les Communautés flamande, française et germanophone, la Région flamande, la Région wallonne, la Région de Bruxelles-Capitale, la Commission communautaire flamande, la Commission communautaire française et la Commission communautaire commune concernant la construction et l'exploitation d'une e-plate-forme commune.*

[2] la capacité qu'ont les systèmes des technologies de l'information et de la communication (TIC), ainsi que les processus de fonctionnement qu'ils permettent, d'échanger des données et de permettre le partage des informations et des connaissances (article 3 de la décision 2004/387/CE) du Parlement européen et du Conseil du 21 avril 2004.

données seront certainement souhaités aussi (en l'occurrence, des données de la DIV sont associées à un fichier géographique du demandeur).

La Commission estime qu'à la lumière de ce qui précède, il est recommandé de prendre des dispositions de manière à permettre non seulement l'accès aux données reprises dans ces banques de données ou leur communication, mais aussi la réalisation d'associations avec celles-ci afin que notamment l'article 4 de la LVP soit respecté de manière optimale. Cela implique l'intervention d'un tiers de confiance ("trusted third party"), par analogie avec le rôle assuré par la Banque-carrefour de la sécurité sociale pour les données qui relèvent de la compétence du Comité sectoriel de la Sécurité Sociale.

Il semble recommandé que Fedict assure un tel rôle en ce qui concerne les données qui relèvent de la compétence du Comité sectoriel pour l'Autorité fédérale. La Commission insiste dès lors pour que Fedict prenne les dispositions nécessaires à cet effet le plus rapidement possible.

A. ÉVALUATION GÉNÉRALE À LA LUMIÈRE DE LA LVP

A.1. Généralités

9. Dans la perspective de la LVP, cet avant-projet représente un pas en avant. A l'occasion du traitement des demandes d'autorisation, les différents comités sectoriels actifs au sein de la Commission ont constaté que de nombreux services fédéraux[3] n'examinent le traitement des données à caractère personnel dans le cadre d'une application d'e-government que dans leur propre perspective et ne tiennent pas ou peu compte du contexte plus vaste dans lequel ce dernier s'inscrit.

10. Il en résulte que leurs applications et leur infrastructure ne sont adaptées qu'à leurs seuls besoins spécifiques. Lorsqu'un service dispose, par exemple, de données à caractère personnel utiles à un autre service, ces données ne sont le plus généralement pas organisées de manière à pouvoir être mises à sa disposition conformément aux exigences de sécurité et de proportionnalité contenues dans la LVP.

11. L'Arrêté Royal du 11 mai 2001 *portant création du Service public fédéral Technologie de l'Information et de la Communication,* qui fixe les missions du Fedict, prévoit pourtant qu'il est, entre

[3] On entend ici par services fédéraux, les services visés à l'article 1er, 10°, de l'avant-projet taxés de "services publics participants".

autres, responsable du développement d'une stratégie commune en matière d'e-government, et de l'assistance à apporter aux services publics fédéraux lors de la mise en œuvre de cette stratégie. Il est aussi chargé de la définition de normes, les standards et architecture de base. Il n'est toutefois pas évident, uniquement sur cette base, d'arriver à ce que l'ensemble du groupe cible agisse de la même manière.

12. Cet avant-projet fait bouger les choses. Dorénavant les Services fédéraux qui souhaitent échanger des données devront se conformer au cadre fixé par l'avant-projet et devront aussi obligatoirement tenir compte du fait qu'ils ne constituent qu'un maillon d'une chaîne.

13. La Commission constate que l'avant-projet délimite clairement le terrain d'action de l'Intégrateur de Services fédéral par rapport à celui des autres intégrateurs de services actifs au niveau fédéral et régional comme la Banque-Carrefour de la Sécurité sociale, la plate-forme eHealth, Easi-Wal, Corve. Son rayon d'action est désormais fixé de telle sorte que tout service public ne dépende plus que de la compétence d'un seul intégrateur de services. L'Intégrateur de Services fédéral n'est compétent que pour 1) les services publics fédéraux qui 2) ne sont pas déjà servis par la Banque-Carrefour de la Sécurité sociale ou la plate-forme eHealth.

14. La Commission estime qu'il faut en effet veiller à ce que les terrains d'action des intégrateurs de services ne se chevauchent pas. Ce point est crucial pour :

- qu'il apparaisse clairement, aussi bien aux services publics concernés qu'à tous ceux qui ne sont pas directement concernés, avec quel intégrateur de services et selon quelles règles il convient de travailler ;
- exclure tout "shopping" entre les différents intégrateurs de services. Ce phénomène de "shopping" pourrait en effet, à terme, avoir des effets néfastes sur la sécurité de d'information. Pour réaliser des économies sur les dépenses, notamment en sécurité de l'information, un service public aurait tendance à travailler avec l'intégrateur de services qui pose le moins d'exigences en la matière. Conséquence : un nivellement par le bas plutôt que par le haut de la sécurité ;
- exclure le risque que plusieurs intégrateurs de services ne se développent en même temps sur le même terrain et ne développent donc des initiatives qui pourraient semer la confusion.

A.2. Intégrateur de services

15. A l'occasion d'une discussion interne sur la problématique de l'intégration, la Commission a mis en avant une série de principes dans le cadre de l'intégration de services. Elle constate que

l'Intégrateur de Services fédéral, tel qu'il est organisé dans le projet, répond aux préoccupations de la Commission dans ce domaine. On peut à cet égard se référer entre autres aux points suivants :

- loyauté, licéité et finalité: voir articles 3, 7, 11, 17, 19 ;
- proportionnalité : voir articles 4, 10, 12, 14, 18 ;
- précision et exactitude : voir article 1 ;
- transparence : voir articles 27 – 32 ;
- sécurité : voir articles 17, 23.

16. L'avant-projet a donc sans aucun doute ses mérites. Cela ne veut cependant pas dire pour autant qu'il ne soulèverait aucun problème ou aucune question par rapport à la LVP. En voici, par article, les points névralgiques et un commentaire s'y rapportant.

B. SUBSIDIAIREMENT : DISCUSSION PAR ARTICLE

Article 2

17. Cet article définit la portée d'une série de termes utilisés dans l'avant-projet.

18. Dans la description du terme intégrateur de services, il est fait mention d'"une instance". La portée de ce terme est vague. Une instance n'est pas nécessairement un service public. Faut-il/peut-on en déduire, par exemple, qu'une entreprise purement commerciale peut être chargée par ou en vertu de la loi d'une telle tâche taxée d'intérêt général?

19. La Commission espère que la réponse à cette question est négative. Par la nature de sa tâche, des masses de données à caractère personnel, parmi lesquelles aussi parfois des données sensibles, seront transmises par l'intégrateur. Ces données ont aussi une valeur commerciale. Le risque que les intérêts commerciaux prévalent par rapport à la tâche d'intérêt général est donc un risque bien réel avec toutes les conséquences qui peuvent en découler, e.a. au niveau de l'intégrité des processus.

20. Le point 4° définit ce qu'il convient d'entendre par donnée authentique. Cette description est importante du fait qu'elle détermine à son tour la définition de ce qu'est une banque de données authentiques.

21. La Commission se rend compte que définir et décrire ce qu'est une donnée authentique n'est pas chose aisée. Idéalement, cette définition doit être suffisamment précise pour que les données pouvant être qualifiées de données authentiques soient claires pour tous. Il faut aussi que cette

définition fasse ressortir que ces données satisfont à une série de conditions de qualité. Des tiers doivent aussi pouvoir les utiliser sans autre examen.

22. Les Pays-Bas ont manifestement choisi d'accorder la qualification de donnée authentique à une donnée particulière par une loi. Ces données authentiques font partie d'un enregistrement de base (source authentique) réglé par la loi[4]. Cette approche offre l'avantage de la transparence mais elle est, par contre, peu flexible.

23. Dans l'avant-projet, on a opté pour une définition générale[5] dans laquelle le caractère authentique n'est pas déterminé par la nature de la donnée mais bien par la manière dont elle est collectée, conservée et mise à disposition sur le réseau. Les éléments déterminants dans ce cadre sont avant tout que la donnée soit collectée et actualisée par une "instance". Ce choix est défendable dans la mesure où, comme on l'a déjà souligné, cette définition permet d'identifier sans équivoque si une donnée est une donnée authentique ou non.

24. La Commission constate que le projet de loi ne comprend aucune autre disposition contenant des indications concrètes concernant l'application de cette définition. Sur la simple base de la définition, elle n'est pas en mesure, pour l'instant, de déterminer quelles données doivent être qualifiées d'authentiques et elle n'est probablement pas la seule dans ce cas. Le fait que seuls des insiders soient capables de déterminer quelles sont les données authentiques témoigne d'un problème de transparence.

25. Le fait que les données soient collectées par un service public ne constitue pas en soi une indication. La définition parle en effet d'"instances". Il s'agit là d'un choix conscient dicté par le fait que des données rassemblées à un endroit unique en dehors des services publics peuvent également constituer un instrument de travail utile. On peut penser, ici, par exemple à la banque de données de l'Ordre des avocats qui reprend les personnes qui ont la qualité d'avocat. Si une application d'e-government ne s'adresse qu'aux avocats, cette banque de données constitue l'instrument idéal pour contrôler si la personne qui s'y connecte est bien un avocat.

---

[4] http ://www.e-overheid.nl/sites/stelselhandboek/wetgeving/wetgeving.html

[5] La définition utilisée dans l'avant-projet, correspond largement à celle qu'on trouve sur le site web de Belgif : *donnée qu'un service public collecte et gère dans une base de données et qui a valeur de donnée unique et originale concernant une personne ou un fait juridique, de sorte que les autres services publics ne doivent plus collecter cette même donnée*[5] mais pour autant qu'on ait pu le constater, cette description n'a pas été approuvée par le législateur. (Belgif = Belgian Government Interoperability Framework : le site des autorités belges placé sous le signe de l'interopérabilité dans le cadre de l'e-government et de la société de l'information ; http ://www.belgif.be/index.php/Authentieke_bron).

26. A la lumière de ce qui précède, puisqu'il ne suffit pas qu'une donnée ait été collectée par une instance pour en garantir le caractère authentique, il faut donc, en vue de l'application de la définition, élaborer une série de critères - dont des critères de qualité - qui permettront d'évaluer si une donnée est réellement une donnée authentique.

27. Toujours dans la même logique, se pose bien sûr la question de savoir qui détermine si une donnée est une donnée authentique ou non, si elle satisfait aux critères de définition d'une donnée authentique et comment le citoyen en est informé, ce qui implique un contrôle et signifie qu'une instance qui collecte des données ne peut pas d'autorité qualifier ses données de données authentiques.

28. Le concept "donnée authentique" demande donc une réflexion plus approfondie.

Article 3

29. Cette disposition stipule que la collecte unique occupe une place centrale dans le cadre du fonctionnement de l'Intégrateur de Services fédéral.

30. La Commission pense pouvoir déduire de la lecture de l'Exposé des motifs et des autres dispositions du projet, que la collecte unique n'est pas élevée, au rang de condition ou d'obligation absolue mais qu'une série de dispositions abondent néanmoins dans ce sens.

31. Le commentaire de l'article 2, 10°, qui définit le public cible de l'Intégrateur de Services fédéral, stipule que les autorités fédérales ne sont pas obligées de faire appel à l'Intégrateur de Services fédéral, de sorte que les dispositions de l'avant-projet ne semblent être pertinentes que pour les autorités qui décident de collaborer avec l'Intégrateur de Services fédéral. Ceci semble en contradiction avec l'article 9 de l'avant-projet qui oblige le détenteur des données authentiques à les mettre à disposition via le réseau. Il serait souhaitable que ce point soit éclairci.

32. L'article 9 de l'avant-projet vise à éviter que des données non authentiques soient collectées à partir du réseau. Cela signifie que les services qui font partie du public cible de l'Intégrateur de Services fédéral seront obligés, dans certains cas, de faire appel à des données stockées ailleurs.

33. La collecte unique n'est pas non plus la panacée. A ce propos, la Commission estime d'ailleurs que le développement d'un système de sources authentiques distinctes qui permet d'éviter le stockage d'importantes quantités de données dans une seule et même banque de données constitue même un plus indéniable par rapport à l'esprit de la LVP. Cela n'empêche toutefois nullement les

tensions qui existent entre d'une part la collecte unique et d'autre part l'article 4, § 1er, 2° de la LVP – *les données collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables*.

34. La collecte unique ne peut pas mener à éluder l'article 4, § 1er, 2° de la LVP. La protection de la vie privée exige le contrôle systématique de la compatibilité par une instance indépendante, in casu les comités sectoriels compétents de la Commission. Il faut, qui plus est, que ce contrôle soit un contrôle effectif et il ne peut donc en aucun cas être ramené à la constatation que le traitement est compatible simplement parce que sans la collecte de ces données le service concerné ne pourrait pas accomplir ses missions.

Article 4 (en combinaison avec les articles 12 et 14)

35. Cet article énonce le principe selon lequel, à défaut de dispositions légales ou réglementaires contraires, l'Intégrateur de Services fédéral ne confère aucun droit complémentaire relatif à la consultation ou la communication de données. Selon l'Exposé des motifs, cela signifie que l'introduction du réseau ne change rien pour les personnes ou services publics instances qui n'ont pas accès aux données ou qui ne sont pas autorisées à le traiter.

36. Ces principes rejoignent ceux à respecter dans le cadre de l'intégration de services mis en avant lors d'une discussion interne sur la problématique de l'intégration qui a eu lieu au sein de la Commission :

- l'intégrateur de services ne peut traiter que les données à caractère personnel pertinentes et non excessives pour les utilisateurs du service intégré ;
- dans le cadre de l'intégration des services, l'intégrateur de services respecte les éventuelles autorisations des comités sectoriels de la Commission ;
- l'intégrateur de services prend les mesures appropriées pour que les utilisateurs des services intégrés n'obtiennent de données à caractère personnel que sur les personnes pour lesquelles ces données sont pertinentes et non excessives par rapport aux finalités légitimes pour lesquelles ils utilisent le service intégré.

37. Selon l'Exposé des motifs, l'article 12 de l'avant-projet prévoit une exception, à savoir quand des données auxquelles le demandeur n'a pas accès sont collectées dans le cadre du calcul d'un résultat d'intégration par le réseau.

38. La Commission estime que dans sa formulation actuelle, l'article 12 constitue une confirmation formelle de ce qui figure dans le commentaire de l'article 4, à savoir que l'utilisation de l'Intégrateur de Services fédéral ne peut pas mener à ce que le demandeur obtienne la consultation et la communication de données qu'il ne pourrait pas obtenir par la consultation directe des banques de données distinctes. Il ne constitue donc pas une exception. Ce point est d'ailleurs étayé par le commentaire de cette disposition. Selon le commentaire de l'article 12, l'article 14, § 2, de l'avant-projet comporte une exception à ces principes.

39. Le fait que l'article 14, § 2, de l'avant-projet constitue une exception aux principes formulés dans les articles 4 et 12 ressort plus qu'à l'évidence. Cette disposition donne l'impression que l'Intégrateur de Services fédéral va chercher des données dans les sources authentiques et les traite au nom d'un demandeur qui ne peut pas obtenir ces données mais auquel est néanmoins communiqué le résultat du traitement. Une telle exception est incompatible avec les exigences des articles 4 et 5 de la LVP.

40. Des contacts ont été établis avec l'auteur de l'avant-projet, afin d'obtenir une explication plus détaillée sur les situations visées par cette disposition. Selon l'explication donnée verbalement, cette disposition vise les situations dans lesquelles un demandeur a besoin d'une information spécifique en vue de l'application d'une disposition légale ou réglementaire mais :

- qu'il n'entre pas en ligne de compte pour avoir accès ou obtenir la communication de cette information à partir de la source authentique concernée ;
- qu'il peut être autorisé à avoir accès ou à obtenir la communication de cette information mais qu'il n'est pas approprié, dans le cadre du respect du principe de proportionnalité, qu'il obtienne tous les détails concernant cette information.

41. La Commission constate que si telle est en effet l'intention de cette disposition, sa formulation est malheureuse. Une exception doit être clairement délimitée afin d'éviter toute discussion sur sa portée. Le texte doit être mieux adapté aux situations d'exception visées. Dans ce cadre, une attention particulière doit être accordée aux conditions essentielles.

42. L'exception postulée mènera le plus souvent à une décision dans le sens de l'article 12*bis* de la LVP. Cela signifie que des mesures adéquates doivent être prévues pour protéger les intérêts légitimes de la personne concernée par la décision. Cette décision doit pouvoir être justifiée en cas de contestation par la personne concernée.

43. L'Intégrateur de Services fédéral n'a toutefois accès à une source authentique ou à une banque de données authentiques que dans la mesure où le demandeur dispose de l'autorisation nécessaire. Si le demandeur ne peut pas obtenir d'autorisation, l'Intégrateur de Services fédéral devra demander une autorisation pour cette opération spécifique. Il serait inacceptable qu'il soit autorisé à décider d'autorité de procéder à une telle action.

44. Il faut également clairement régler ce que conservera l'Intégrateur de Services fédéral dans le cadre d'une telle intervention et combien de temps il le conservera. En principe, il ne traite pas de données et ne les stocke pas non plus.

45. Il ne semble pas recommandé, à l'article 11, de prendre pour critère les banques de règles. Etant donné que ces dernières constituent la traduction technique des règles juridiques d'applications à ces données et à l'accès à ces données, il vaut mieux se référer aux dispositions légales ou réglementaires.

Article 5

46. Le § 1er stipule que les services publics fédéraux participants et les intégrateurs de services communiquent par voie électronique à l'Intégrateur de Services fédéral toute donnée électronique disponible dont il a besoin pour l'exécution de sa mission d'intégration de services. La Commission en déduit que l'Intégrateur de Services fédéral est autorisé, dans le cadre de sa tâche d'intégration de services, à avoir accès à toutes les banques de données – et donc aussi aux données qui y sont stockées – qui font partie du réseau. Il s'agit là d'une dérogation au principe d'autorisation prévu, e.a. à l'article 36*bis* de la LVP et à l'article 5 de la LRN.

47. La Commission comprend qu'il serait très compliqué d'exiger de l'Intégrateur de Services fédéral qu'il demande une autorisation distincte pour chaque banque de données. Elle constate d'ailleurs que l'avant-projet offre en contrepartie des garanties contre les abus du chef de l'Intégrateur de Services fédéral :

- l'autorisation n'est valable que pour 1 seule finalité, à savoir l'intégration de services (article 5) ;
- il ne peut demander/consulter les données qu'au nom d'un demandeur qui dispose de l'autorisation exigée (article 10 de l'avant-projet) ;
- le développement de cercles de confiance (article 17 de l'avant-projet) qui garantissent une totale transparence end-to-end.

48. Conformément au § 2 de cet article, l'Intégrateur de Services fédéral communique par voie électronique aux services publics participants et aux autres intégrateurs de services les données disponibles dont ils ont besoin pour exécuter leurs missions.

49. En soi, cette disposition peut donner l'impression que tout service public participant peut, sans plus, obtenir les données dont il a besoin par le biais de l'Intégrateur de Services fédéral. La Commission constate que cette disposition doit bien entendu être lue avec le texte des articles 4, 10, 12, 14 et 18 de l'avant-projet en tête. Cela signifie que le destinataire peut en effet obtenir les données dont il besoin, pour autant qu'il dispose de la/des autorisation(s) nécessaire(s) à cet effet.

Article 7

50. Cet article décrit les missions de l'Intégrateur de Services fédéral.

51. La Commission constate que celles-ci sont axées sur l'encadrement sûr, univoque, transparent et technique du processus d'intégration mais émet néanmoins la remarque suivante: la transformation des banques de données en sources authentiques est considérée comme une mission expresse de l'Intégrateur de Services fédéral. La Commission renvoie à ce sujet aux remarques qu'elle a déjà faites concernant la description de la donnée authentique.

Article 8

52. Cet article accorde à l'Intégrateur de Services fédéral le droit d'utiliser le numéro d'identification du Registre national pour l'exécution de sa mission. A titre de justification, l'Exposé des motifs invoque le fait que ce numéro constitue le moyen le plus simple et le plus sûr de relier entre elles les banques de données afin d'obtenir les différentes données relatives à une même personne.

53. La Commission constate que le public cible de l'Intégrateur de Services fédéral est très hétérogène et comprend indéniablement des services qui traitent des données sensibles au sens des articles 6 à 8 de la LVP dans des banques de données. On peut faire référence ici, à titre d'illustration au casier judiciaire central (article 8 de la LVP) – sans doute une source authentique - une banque de données gérée par le Service public fédéral Justice. Ce dernier est également responsable du paiement des ministres des cultes (article 6 de la LVP) et gère aussi les dossiers des détenus qui contiennent souvent, outre des informations judiciaires, également des informations médicales (article 7 de la LVP).

54. En ce qui concerne la problématique de l'utilisation du numéro d'identification du Registre national et les problèmes des données sensibles et des éventuelles connexions qui peuvent y être liées, la Commission renvoie à son avis n° 14/2008 du 2 avril 2008 relatif à un projet de loi *portant institution et organisation de la plate-forme eHealth*, dans lequel elle a conclu que l'utilisation du numéro d'identification pouvait être acceptée à condition que d'autres techniques de protection des données à caractère personnel soient appliquées:

- pas de stockage central : article 3 de l'avant-projet ;
- condition d'autorisation par un comité sectoriel : article 10 de l'avant-projet ;
- conseiller en sécurité : article 23 de l'avant-projet.

55. L'avant-projet ne contient aucune disposition relative à la constitution de répertoires de références. Si le but est de constituer des répertoires de références, étant donné qu'il a été montré plus avant que des données sensibles peuvent y figurer, il est recommandé de le prévoir expressément et par analogie avec ce qui est prévu pour la plate-forme eHealth, d'également prévoir, pour sa concrétisation, une demande d'avis préalable du Comité sectoriel pour l'Autorité Fédérale.

56. La Commission constate une différence entre le texte de l'article 8 proposé et son commentaire. Selon l'explication : "*Ce droit est une autorisation générale d'utiliser le numéro d'identification dans toutes les banques de données connectées au réseau. L'article 8 constitue de ce fait une dérogation formelle au principe d'autorisation dont il est question à l'article 8 de la loi du 8 août 1983.*".

57. Si l'objectif est que tous les services publics réellement participants soient autorisés à utiliser le numéro d'identification dans les banques de données qu'ils mettent sur le réseau, il faut le dire clairement. La formulation actuelle du texte ne vise exclusivement que l'Intégrateur de Services fédéral à proprement parler.

58. La Commission ne voit cependant aucune raison pour laquelle les services publics participants dérogeraient au principe d'autorisation ancré à l'article 8 de la loi du 8 août 1983. Il vaudrait mieux faire de l'obtention d'une autorisation une condition préalable à l'intégration dans le réseau, comme c'est d'ailleurs aussi le cas pour certaines instances qui veulent adhérer au réseau de la sécurité sociale[6].

[6] Voir article 4 de l'Arrêté Royal du 16 janvier 2002 *relatif à l'extension du réseau de la sécurité sociale à certains services publics et institutions publiques des Communautés et des Régions, en application de l'article 18 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.*

Article 9

59. Voir la problématique de la collecte unique : article 3.

Article 10

60. Cet article postule le principe de l'autorisation préalable par le comité sectoriel compétent pour toute communication de données à caractère personnel dans le cadre d'une intégration de services.

61. Vu le fonctionnement actuel des comités sectoriels, cela signifie qu'un service intégré peut mener à devoir introduire un dossier auprès de plusieurs comités sectoriels (=procédure lourde). Il n'est pas exclu, non plus, que ces différents comités sectoriels prennent des décisions divergentes.

62. La Commission ne peut qu'être d'accord. Elle attire toutefois l'attention sur le fait qu'elle dispose d'une série d'instruments destinés à contribuer à ce que les différents comités n'adoptent pas de points de vue contradictoires dans un même dossier, mais elle admet qu'ils ne sont pas idéaux et que les choses dépendent fortement de la reconnaissance en temps opportun du caractère supra-sectoriel des problèmes.

63. Que la Commission ait la possibilité, en cas d'intégration de services, de déroger à la répartition légale des compétences entre les différents comités sectoriels en confiant la décision relative à toutes les autorisations nécessaires dans le cadre du dossier à 1 seul comité/ à plusieurs comités réunis / à la Commission n'est pas une mauvaise chose.

64. La tâche des comités sectoriels et de la Commission consiste à veiller à ce que les traitements ultérieurs soient exécutés conformément à la LVP. Actuellement, le comité sectoriel appelé à se prononcer sur une demande d'autorisation ne dispose que d'une vision tronquée qui ne lui permet pas d'avoir connaissance de tous les points sensibles par rapport à la LVP. Le fait de confier un “dossier d'intégration” dans son intégralité à un seul comité/ à plusieurs comités siégeant en session conjointe / à la Commission permettra de mieux pouvoir en évaluer l'impact sur la vie privée.

65. Un point non négligeable est que cela permet aussi de rassembler l'expertise des membres de plusieurs comités sectoriels, ce qui n'est pas du luxe dans les "dossiers d'intégration" complexes.

66. Par souci d'exhaustivité, la Commission fait remarquer que le fait que l'article 10 de l'avant-projet lui donne carte blanche pour prendre les dispositions nécessaires en la matière, n'enlève rien au flou qui persiste au niveau de toute une série de problèmes de procédure. Chaque comité

sectoriel est obligé de demander l'avis technique et juridique de l'institution de gestion concernée. Quelle(s) institution(s) de gestion va(on)t-elle(s) émettre un avis dans un "dossier d'intégration" ? Dans l'hypothèse de l'attribution d'un “dossier d'intégration” au Comité sectoriel du Registre national, les services du Registre national doivent-ils, eux aussi, se pencher sur les données qui se trouvent à la DIV ou à l'ONEM ?

67. Il semble à cet égard recommandé d'opter pour que l'institution de gestion du comité sectoriel désigné soit chargé de la rédaction de l'avis juridique et technique, ceci toutefois en concertation avec les institutions de gestion des autres comités sectoriels qui auraient normalement dû être impliqués dans le dossier. S'il devait être décidé de faire traiter le dossier par plusieurs comités sectoriels conjointement, en ce qui concerne les institutions de gestion, la même procédure pourrait être appliquée aux institutions de gestion.

68. L'institution de gestion dispose d'un délai de 15 jours pour émettre un avis juridique et technique (article 31*bis*, § 3, premier alinéa de la LVP). Si le nouveau système prévoit une concertation avec une autre institution de gestion, un délai de 15 jours est trop court pour le faire de manière sérieuse. Il vaudrait donc mieux prévoir un délai mieux adapté, par exemple de 30 jours.

Article 15

69. Selon les explications données verbalement, cette disposition vise à permettre à l'Intégrateur de Services fédéral de demander les données au nom d'un service public dûment autorisé lorsque ce dernier ne dispose pas des techniques de l'information lui permettant de le faire lui-même et d'ensuite les remettre au service public autorisé sous la forme / dans le format qui lui permettra de les traiter.

70. S'il s'agit bien là de l'objectif de cette disposition, le texte de cet article devrait être mieux expliqué.

71. La Commission comprend bien que tous les services publics ne disposent pas immédiatement de toute l'infrastructure informatique nécessaire pour extraire des données à partir de sources authentiques via l'Intégrateur de Services fédéral mais qu'ils doivent néanmoins avoir la possibilité d'obtenir les données pour lesquelles ils ont obtenu une autorisation d'accès ou de communication. Dans ce cas, l'Intégrateur de Services fédéral interviendrait en qualité de sous-traitant pour le compte du responsable du traitement.

Article 16

72. Cet article stipule que les données échangées par le biais de l'Intégrateur de Services fédéral sur un support papier ont une force probante identique jusqu'à preuve du contraire.

73. Cette disposition ne soulève aucune remarque particulière en ce qui concerne la LVP. Il est toutefois constaté ce qui suit :

- la donnée authentique pèse lourd sur l'application de cette disposition et la Commission fait aussi référence aux remarques qu'elle a formulées à ce propos (voir article 2) ;
- la communication des données sur lesquelles reposent la décision et la source de ces données (transparence) doivent absolument être communiquées à l'intéressé dans le cadre de la décision pour lui permettre de prouver le contraire le cas échéant.

Article 17

74. Cette disposition opte pour le développement de "cercles de confiance" en vue d'assurer la sécurisation des données, une option que la Commission semble manifestement approuver si l'on en croit la discussion interne consacrée à la problématique de l'intégration.

75. Ces cercles de confiance sont développés pour protéger les données du citoyen. Ils sont toutefois peu tangibles pour le citoyen et ne lui inspirent donc pas directement confiance. Dans cette optique, la Commission plaide pour que l'avant-projet contienne aussi des mesures destinées à augmenter leur transparence pour le citoyen. Concrètement, cela suppose, entre autres, que le citoyen dispose, par analogie avec le Registre national, par principe, du droit de vérifier, par le biais de l'Intégrateur de Services fédéral, quelles personnes/instances ont consulté ses données dans les sources authentiques[7].

Articles 20 à 26

76. Ils traitent d'autres facettes de la protection des données, notamment du secret professionnel, de la destruction des banques de données, du conseiller en sécurité.

[7] Voir article 6, § 3, deuxième alinéa, 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.*

77. La Commission constate que si ces dispositions ne sont pas reprises littéralement, elles s'inspirent néanmoins largement des dispositions de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* et l'Arrêté Royal du 12 août 1993 *relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale*.

78. Que l'Intégrateur de Services fédéral et les services publics participants aient l'intention de travailler sur la base des mêmes principes de sécurité n'a rien d'étonnant : ces principes ont depuis longtemps prouvé leur légitimité dans le cadre du réseau de la sécurité sociale. Dans la perspective de la LVP, cela ne semble pas être une mauvaise chose. Gérer des réseaux sur la base de différentes perceptions en matière de sécurité de l'information augmente le risque d'incidents de sécurité du fait notamment qu'il est beaucoup plus difficile, dans ce cas, d'identifier les maillons faibles de la chaîne de sécurité.

79. Il semble toutefois recommandé d'ajouter quelques précisions à ce volet :

- l'article 20 qui traite du secret professionnel et se limite aux données auxquelles le secret professionnel s'applique en vertu d'une disposition réglementaire d'un groupe professionnel. Cette formulation donne l'impression de laisser la voie ouverte au traitement moins strict de toutes les autres données. Pour ne pas créer de malentendu à ce niveau, il est recommandé, par analogie avec l'article 12, § 2, 2° de la loi du 8 août 1983, de faire signer à toutes les personnes chargées du traitement de données à caractère personnel, quelle qu'en soit la nature, une déclaration par laquelle elles s'engagent à préserver le caractère confidentiel des informations et à ne les utiliser exclusivement que pour les finalités prévues dans l'autorisation. En cas de constatation d'incidents de sécurité, une telle déclaration empêchera que l'intéressé d'invoquer l'imprécision ou l'ignorance.

- L'article prévoit que l'identité du conseiller en sécurité doit être communiquée au comité sectoriel compétent. Dans la formulation actuelle de l'avant-projet, cela signifierait que le rôle du comité serait limité à prendre acte du nom de la personne désignée. Cela signifie-t-il que le Comité sectoriel du Registre national serait désormais obligé d'accepter sans plus le conseiller en sécurité dont la désignation est rendue obligatoire en vertu de l'article 8 de la loi du 8 août 1983 *organisant un Registre national des personnes physiques ?*

Une déclaration du même type au Comité sectoriel de la Sécurité sociale et de la Santé est également prévue au sein du réseau de la sécurité sociale, mais dans ce cas il est prévu que ce comité émette un avis sur le caractère approprié de cette personne.

Il est donc recommandé de prévoir pour tous les comités sectoriels la possibilité d'apprécier le caractère approprié du conseiller en sécurité proposé, ce qui n'est actuellement pas évident pour le Comité sectoriel pour l'Autorité Fédérale sur la base de la législation actuelle.

- Dans le texte en français des articles 23 à 26 on trouve les termes "consultant en sécurité". Il vaudrait mieux utiliser les mêmes termes que dans l'Exposé de motifs, à savoir les termes "conseiller en sécurité".

- En ce qui concerne l'Arrêté Royal qui fixe les règles selon lesquelles le conseiller en sécurité exerce ces missions, il est recommandé de prévoir une demande d'avis de la Commission par analogie avec ce qui est prévu à l'article 17*bis* de la LVP en ce qui concerne le préposé à la protection des données.

C. CONCLUSIONS

80. La Commission constate que l'Intégrateur de Services fédéral, mais aussi le Comité de concertation des intégrateurs de service disposent de vastes compétences, entre autres, en ce qui concerne la qualification des données authentiques et partant l'extension des sources authentiques et les mesures de sécurité. La Commission pense qu'il est recommandé qu'étant donné l'impact de ces mesures, une série d'interventions, notamment la problématique de la qualification des données authentiques, soient réglées de préférence par un Arrêté Royal soumis pour avis à la Commission.

81. En ce qui concerne les dispositions pénales, pour être tout à fait complète, la Commission attire l'attention sur ce qui suit :

- La majorité des dispositions pénales ne visent que les personnes physiques et ne concernent pas les personnes morales ;
- Il existe un déséquilibre entre la lourde peine prévue pour un fonctionnaire (article 45) et le délai de prescription de l'action pénale plutôt court (article 46).

PAR CES MOTIFS,

la Commission

émet un avis favorable à condition qu'il soit tenu compte des remarques formulées plus avant concernant :

- la délimitation claire du champ d'application de l'intégrateur de services fédéral par rapport aux autres intégrateurs de services telle qu'elle est prévue, doit être conservée de sorte que chaque service public ne puisse réellement ne recourir qu'à un seul intégrateur de services : points 13-14 ;
- la portée du terme "instance" dans la définition de l'intégrateur de services : points 18-19 ;
- la définition des données authentiques : points 24-28 ;
- des contrôles effectifs de compatibilité : point 34 ;
- l'article 14, § 2 : points 39-45 ;
- les répertoires des références : point 55 ;
- la dérogation au principe d'autorisation de l'article 8 de la loi du 8 août 1983 : point 58 ;
- l'avis technique et juridique : point 66 ;
- les éclaircissements concernant l'article 15 : points 67-68;
- la transparence : point 75 ;
- la sécurité : point 79 ;
- le rôle du Roi : point 80.

Etant donné l'importance de l'avant-projet soumis pour avis, la Commission se tient à disposition dans le cadre de toute éventuelle nouvelle révision et/ou exécution des dispositions de l'avant-projet.

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

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere