Octobre 2007

Mise en œuvre de la révision LAVS du 23 juin 2006 (Nouveau numéro d'assuré AVS)

Commentaire de l'ordonnance du DFI sur les exigences minimales auxquelles doivent satisfaire les mesures techniques et organisationnelles à prendre par les services et institutions utilisant systématiquement le numéro d'assuré AVS en dehors de l'AVS

1 Contexte

Le Parlement a décidé le 23 juin 2006 une révision de la LAVS (nouveau numéro d'assuré AVS)[1], qui doit entrer en vigueur le 1er décembre 2007. Elle ne concerne pas que l'AVS, mais aussi d'autres utilisateurs du nouveau numéro : la catégorie de ces autres utilisateurs habilités est définie, et le nouvel art. 50*g*, al. 2, let. a, LAVS exige d'eux qu'ils prennent « des mesures techniques et organisationnelles pour que le numéro AVS utilisé soit correct et qu'il n'en soit pas fait une utilisation abusive ». L'art. 50*g*, al. 3, fait obligation au Département fédéral de l'intérieur de définir, d'entente avec le Département fédéral des finances, les exigences minimales auxquelles doivent satisfaire ces mesures. Ces normes doivent faire l'objet d'une ordonnance distincte.

[1] FF 2006 5505

2 Commentaire des différentes dispositions

2.1 Section 1 – Dispositions générales

Les art. 1 et 2 servent à clarifier le but visé par le nouveau texte législatif et à en délimiter le champ d'application. La teneur des art. 1 et 2, al. 1, suit de près le mandat donné par le législateur :

- l'art. 1 consiste en une simple disposition visant à garantir que les numéros d'assuré utilisés soient corrects et à en éviter toute utilisation abusive ;
- l'art. 2, al. 1, clarifie le champ d'application de l'ordonnance : celle-ci, conformément à la systématique de la loi à laquelle elle est subordonnée, n'est applicable qu'aux utilisateurs du numéro d'assuré en dehors de l'AVS, l'assurance elle-même étant régie par la LAVS. De ce fait, les employeurs en tant qu'organes de l'AVS sont soumis à la loi et non à l'ordonnance. L'al. 2 tient compte du fait qu'il est pratiquement inutile de prendre des mesures de précaution relativement à l'exactitude du numéro lorsqu'il n'y a pas gestion active d'une collection de données. En pareil cas – par exemple pour une analyse statistique fondée sur des extraits non dynamiques de registres – on ne procède à aucune mutation et il n'y a pas lieu de s'attendre à une diffusion ultérieure du numéro, ni donc à des dommages encourus par d'autres utilisateurs externes si le numéro n'est pas correct. Les seules normes à respecter dans ces cas sont celles qui servent à prévenir toute utilisation abusive du numéro.

2.2 Section 2 – Mesures visant à garantir l'utilisation du numéro d'assuré correct

La section 2 traite des mesures visant à garantir l'utilisation du bon numéro d'assuré. Elles ne concernent que les utilisateurs qui se servent du numéro d'assuré dans des collections de données.

L'art. 3 pose une exigence que doit remplir le système électronique dans son ensemble: tant l'architecture de la base de données que les programmes et les dispositifs d'application doivent être conçus de telle sorte qu'aucun doute ne puisse surgir :

- sur la personne auquel le numéro est attribué, ni sur le numéro attribué à cette personne,
- ni, si plusieurs numéros correspondent à la même personne, sur celui qui est actuellement valable. Cette distinction est particulièrement nécessaire dans les systèmes qui gardent un historique des données. Seule une désignation sans équivoque du champ de données contenant le numéro d'assuré actuellement valable – relié sans équivoque aux données correspondantes de la personne assurée – permettra de procéder à la vérification nécessaire pour garantir la correction du numéro d'assuré utilisé.

L'art. 4 exige qu'un programme de vérification de la clé de contrôle soit installé sur les systèmes prévoyant la saisie manuelle du numéro d'assuré, afin de prévenir les fautes d'inattention lors de la saisie. Comme des erreurs de saisie peuvent aussi survenir avec le recours à la technique du code barre – suivant la provenance de ce dernier –, un programme semblable doit également être installé dans ce cas-là. Cette vérification n'est plus nécessaire, en revanche, lors de l'utilisation d'une bande magnétique ou d'une puce à microprocesseurs, procédés prévus pour la carte d'assuré dans l'assurance-maladie. La clé de contrôle et le moyen de la vérifier sont décrits en détail dans l'annexe 1. En pratique, les mesures exigées à l'art. 4 doivent pouvoir être appliquées de façon simple au moyen de logiciels disponibles dans le commerce.

2.2.1 Art. 5 – Sûreté de la source des données saisies

Etant donné les bases légales y afférentes, il est plus que probable que le numéro d'assuré AVS sera utilisé de manière systématique dans d'autres assurances sociales, ainsi que dans divers domaines de l'administration. Plus il y aura d'utilisateurs hors AVS, et plus ils recourront dans leurs échanges de données au numéro d'assuré AVS en tant qu'élément d'attribution décisif, plus il sera important que le numéro utilisé soit le bon. Afin de prévenir les risques les plus importants liés à la diffusion de mauvais numéros, l'art. 134^{quinquies} RAVS prévoit déjà une réglementation spéciale relative à la première mise à jour complète des fichiers électroniques consécutive à l'introduction du numéro d'assuré, ainsi qu'à la vérification des numéros d'assuré.

L’al. 1, faisant appel à la responsabilité de l’utilisateur, exige de lui qu’il ne saisisse des numéros d’assuré dans des collections de données que s’il est suffisamment sûr que ces numéros sont corrects ; l’utilisateur est invité à apprécier le cas sur la base des circonstances concrètes : les al. 2 et 3 lui fournissent des repères concrets pour une pratique responsable dans la saisie des numéros. Il peut être certain de ne pas enfreindre les standards minimaux s’il organise la saisie en tenant compte de ces indications. Il n’en reste pas moins libre de trouver une solution sous sa propre responsabilité. L’al. 4 autorise la CdC à publier une liste de sources de données recommandées. Cette mesure facilite aux utilisateurs l’accès à des sources d’information sûres.

2.3 Section 3 – Mesures visant à prévenir toute utilisation abusive

2.3.1 Art. 6 – Principes

L’al. 1 énonce les principes concernant la restriction d’accès et l’autorisation d’accès aux données (sur des supports physiques ou dans des fichiers électroniques) applicables à tous les utilisateurs ; l’al. 2, lui, ne concerne que les utilisateurs exploitant des systèmes complexes. Est considéré comme complexe, p. ex., un système qui exploite simultanément plusieurs bases de données, ou dans lequel plusieurs programmes utilisateurs accèdent à la même base de données, ou encore dans lequel l’application est employée par un grand nombre d’utilisateurs. Ce type d’exploitation implique en pratique, dans l’intérêt même de l’exploitant, une analyse régulière des risques, laquelle doit toujours prendre en considération, entre autres facteurs, la nécessité de protéger le numéro d’assuré et la problématique du regroupement illicite de bases de données. Une manière de tenir compte de cette problématique pourrait être, dans les systèmes qui exploitent plusieurs banques de données dont chacune contient le numéro d’assuré, de coder dans chacune le numéro différemment, de manière à empêcher même les administrateurs de systèmes de regrouper ces bases de données illicitement. Les mesures à prendre sont fonction des résultats de l’analyse des risques. Au reste, tous les utilisateurs – même les petits cabinets médicaux, p. ex. – doivent à tout le moins, conformément à l’al. 3, respecter les normes de sécurité décrites dans l’annexe 2.

2.3.2 Art. 7 – Transmission de données par des réseaux publics

Lorsque des données transitent par des réseaux publics, il existe un risque élevé qu’elles tombent en possession de personnes à qui elles ne sont pas destinées. Est considéré comme public tout réseau qui n’est pas réservé à un groupe exhaustivement défini d’utilisateurs soumis à un contrôle d’accès particulier (p. ex. l’Intranet d’un service). Il est possible de parer audit risque en recourant aux possibilités techniques actuelles de cryptage.

2.3.3 Art. 8 – Utilisation et communication

Une protection effective contre les abus implique que le numéro d’assuré ne soit utilisé que par des services et institutions habilités à le faire. Quiconque l’utilise sans autorisation commet un délit au sens de l’art. 87 LAVS. Mais un emploi abusif peut aussi être le fait d’un service ou d’une institution autorisés à utiliser le numéro d’assuré de manière systématique. Ce risque se présente en particulier lorsque le numéro est utilisé à d’autres fins que l’exécution des tâches prévues ou qu’il est transmis à des tiers de manière non autorisée. Les utilisateurs habilités y pareront en veillant à informer dûment leur personnel, dans les cours de formation et de perfectionnement, de manière à ce qu’il n’utilise le numéro que pour remplir ses tâches et ne le communique qu’en conformité avec les prescriptions légales. A cet égard, il conviendra de toujours se référer à celles qui concernent la communication de données et s’appliquent au type d’activité concerné.

3 Annexes 1 et 2

L’annexe 1 décrit en détail la logique de la clé de contrôle à vérifier conformément à l’art. 4 ; l’annexe 2 énonce les normes minimales de sécurité à respecter dans l’exploitation de ressources informatiques et d’unités de mémoire employés en lien avec l’utilisation systématique du numéro d’assuré. Commes ces annexes parlent d’elles-mêmes, elles n’ont donc pas besoin d’autre commentaire, hormis le ch. 5 de l’annexe 2.

3.1 Annexe 2, ch. 5

Le ch. 5 prévoit que les activités et événements importants soient consignés et analysés régulièrement. Ces activités et événements comprendront, suivant la forme concrète du système, des processus divers, dont il n'est pas possible de dresser une liste exhaustive valable pour tous les utilisateurs. Nous nous contenterons de mentionner à titre d'exemples :

- lancement et arrêt du système,
- demande de connexion,
- tentatives avortées d'authentification,
- échecs de tentatives d'accès,
- octroi et modification de privilèges,
- toute action nécessitant des privilèges élevés.