Projet de juin 2007

Paquet n° 2
Mise en œuvre de la révision LAVS du 23 juin 2006 (Nouveau numéro d'assuré AVS)

Commentaire de l'ordonnance sur les standards minimaux auxquels 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 janvier 2008 au plus tard. 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

[1] FF 2006 5505

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 standards minimaux auxquels doivent satisfaire ces mesures. Ces normes doivent faire l'objet d'une ordonnance distincte.

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. Leur teneur suit de près le mandat donné par le législateur :

- l'ordonnance se borne, à l'art. 1, à des dispositions visant à garantir que les numéros d'assuré utilisés soient corrects et à en éviter toute utilisation abusive ;
- l'art. 2 clarifie le champ d'application de l'ordonnance : celle-ci n'est applicable, conformément à la systématique de la loi, 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.

2.2 Section 2 – Spécifications techniques

La section 2 traite de détails techniques relatifs aux fichiers de données électroniques. D'une part, les numéros d'assuré ne peuvent être mémorisés qu'à un seul endroit dans une même banque de données (art. 3), car il faut que l'on sache à coup sûr où procéder aux corrections qui s'avéreraient nécessaires. D'autre part, 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 également survenir avec le recours à la technique du code barre – suivant la provenance de ce dernier –, le même programme doit être installé dans ce cas-là. La clé de contrôle et le moyen de la vérifier sont décrits en détail dans l'annexe 1.

En pratique, les mesures exigées à la section 2 doivent pouvoir être appliquées de façon simple au moyen de logiciels disponibles dans le commerce.

2.3 Section 3 – Mesures visant à garantir l'utilisation du bon numéro d'assuré

Etant donné les bases légales, 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. Il existe ici des différences d'échelle : de faux numéros dans un système administratif fermé ou dans une petite base de données n'ont pas les mêmes conséquences que s'ils se trouvent dans des systèmes utilisant de grandes bases de données ou ayant de fréquentes répercussions à l'extérieur. L'ordonnance tient compte de cette différence de risques en réglementant différemment les exigences minimales tant en ce qui concerne la saisie du numéro que sa vérification.

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

Art. 5, al. 1

La 1re phrase de cette disposition ne se réfère qu'à la *première mise à jour complète* des fichiers de données électroniques comprenant le numéro d'assuré et elle exige que ne soient enregistrés que les numéros d'assuré communiqués (et attribués) par la Centrale de compensation (CdC). L'obligation de demander les numéros d'assuré à la CdC dans le contexte de la première mise à jour complète ne s'applique qu'au groupe limité d'utilisateurs qui ont des effets très importants à l'extérieur, ou qui gèrent des bases de données très volumineuses, et qui de ce fait présentent de plus grands risques.

En font notamment partie, outre les assureurs-maladie au sens de la LAMal, les services tenant des registres visés par l'art. 2 de la loi sur l'harmonisation de registres (RS 431,02). Sont précisément concernés :

- le registre informatisé de l'état civil (Infostar), tenu par les cantons et exploité par l'Office fédéral de la justice ;
- le système d'information central sur la migration (SYMIC) de l'Office fédéral des migrations ;

  tant Infostar que SYMIC collaborent avec la CdC pour l'attribution des numéros ; des données relatives à l'AVS sont également échangées p. ex. en lien avec des prestations (annonces de décès par Infostar) ou avec le remboursement de cotisations (départs à l'étranger) ;

- d'autres systèmes d'information du Département fédéral des affaires étrangères, comme VERA et Ordipro (Administration en réseau des Suisses de l'étranger), ainsi que le rôle d'immatriculation des représentations diplomatiques et consulaires suisses à l'étranger ;

- les registres cantonaux et communaux des habitants, ainsi que ceux des électeurs, lorsqu'ils servent aux élections populaires et aux élections du Conseil national ; il est particulièrement important que les numéros d'assuré inscrits dans ces registres soient corrects, puisque toute la population y est enregistrée et que ces instruments administratifs jouent un rôle essentiel dans la collectivité.

La 2e phrase se réfère aux « autres saisies », qui comprennent notamment les saisies à effectuer dans les banques de données des assureurs-maladie ou dans les registres après la première mise à jour complète, donc dans le cadre des « affaires courantes » (p. ex. quand une personne change de caisse-maladie ou s'installe dans une autre commune). Dans ces cas, les mêmes normes de sécurité doivent s'appliquer que pour les autres services et institutions en général.

Al. 2 à 5
L'al. 2 exige de l'utilisateur, en faisant appel à sa responsabilité propre, qu'il ne saisisse des numéros d'assuré dans des fichiers électroniques que s'il est suffisamment sûr que ces numéros sont corrects, l'utilisateur étant invité à apprécier le cas sur la base des circonstances concrètes ; les al. 3 et 4 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 sa propre solution pour évaluer la sûreté de la source au sens de l'al. 2. L'al. 5 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.

2.3.2 Art. 6 – Vérification

Seuls devraient en principe être tenus de vérifier régulièrement l'exactitude des numéros d'assuré contenus dans leurs bases de données les services et institutions qui ont déjà été tenus de demander ces numéros à la CdC à l'occasion de leur première mise à jour complète. Une fois ce processus achevé, les modifications courantes doivent être effectuées suivant les prescriptions de l'art. 5, al. 2 à 4. Pour donner un exemple pratique, un assureur-maladie disposera de cette manière de données correctes à sa première mise à jour complète. Mais si des modifications surviennent ensuite en raison de changements de caisse, le numéro des nouveaux assurés pourra p. ex. être saisi à partir de la carte d'assuré encore valable émise par l'assureur précédent (avec un contrôle complémentaire de l'identité, p. ex. au moyen d'une copie de la carte d'identité). A la longue, des erreurs de saisie peuvent survenir dans des fichiers où les modifications sont fréquentes. Pour que ces erreurs puissent être corrigées et pour éviter qu'elles ne se répercutent plus loin, les services et institutions pour lesquels les risques potentiels sont plus grands sont tenus, par l'art. 6, al. 1, de vérifier périodiquement la concordance de leurs données avec celles de la CdC.
La même obligation doit s'appliquer, en vertu de l'al. 2, même à des services et institutions non encore connus, s'il est à craindre qu'ils utilisent une quantité de numéros incorrects susceptible de compromettre l'application de l'AVS ou le fonctionnement normal d'autres utilisateurs. C'est pourquoi l'al. 2 prévoit que la CdC est habilitée à ordonner des vérifications.

2.4 Section 4 – Mesures visant à prévenir toute utilisation abusive

2.4.1 Art. 7 – 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 dans lequel plusieurs programmes utilisateurs accèdent à la même banque de données ou 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, qui doit toujours prendre en compte entre autres facteurs la nécessité de protéger le numéro d'assuré. Les mesures à prendre sont fonction des résultats. Les autres utilisateurs, p. ex. les petits cabinets médicaux, doivent à tout le moins, conformément à l'al. 3, respecter les normes de sécurité décrites dans l'annexe 2.

2.4.2 Art. 8 – 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. Il est possible de parer à ce risque en recourant aux possibilités techniques actuelles de cryptage.

2.4.3 Art. 9 – 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 prescriptions minimales de sécurité à respecter dans l'exploitation de ressources informatiques et de supports de données employés en lien avec l'utilisation systématique du numéro d'assuré. Elles parlent d'elles-mêmes et 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.