Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

19.057

Message relatif à la modification de la loi fédérale sur l'assurance-vieillesse et survivants

(Utilisation systématique du numéro AVS par les autorités)

du 30 octobre 2019

Madame la Présidente,
Monsieur le Président,
Mesdames et Messieurs,

Par le présent message, nous vous soumettons le projet d'une modification de la loi fédérale sur l'assurance-vieillesse et survivants, en vous proposant de l'adopter.

Simultanément, nous vous proposons de classer l'intervention parlementaire suivante:

2017 P 17.3968 Concept de sécurité pour les identifiants des personnes (N 19.09.18 Commission des affaires juridiques)

Nous vous prions d'agréer, Madame la Présidente, Monsieur le Président, Mesdames, Messieurs, l'assurance de notre haute considération.

30 octobre 2019

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Ueli Maurer
Le chancelier de la Confédération, Walter Thurnherr

Condensé

L'utilisation contrôlée du numéro AVS (NAVS) doit permettre d'accroître l'efficacité des processus administratifs. À l'avenir, il faut que les autorités de la Confédération, des cantons et des communes puissent, de manière générale, utiliser systématiquement le NAVS pour accomplir leurs tâches légales. Cela permettra d'éviter des confusions lors du traitement de dossiers personnels, tout en contribuant à la mise en œuvre de la stratégie suisse de cyberadministration et en renforçant l'efficience administrative.

Contexte

Depuis sa création en 1948, l'AVS utilise un numéro d'assuré. À ce jour, cet identificateur de personnes a pour objectif de faciliter le traitement des informations concernant les cotisations et le calcul des prestations des assurances sociales. Un nouveau numéro AVS à treize chiffres, non parlant, a été introduit en 2008 et les conditions de son utilisation systématique ont été précisées à cette occasion. Depuis lors, l'utilisation systématique du NAVS en dehors de l'AVS est seulement autorisée à certaines conditions. Elle l'est, d'une part, pour les services et institutions chargés de l'exécution du droit cantonal dans un domaine lié aux assurances sociales. Elle l'est, d'autre part, si une disposition spécifique d'une loi spéciale fédérale ou cantonale l'autorise en définissant le but de l'utilisation et les utilisateurs légitimés. Cela permet dans chaque cas le contrôle démocratique.

Dans le traitement des données, l'utilisation systématique du NAVS en tant qu'identificateur de personnes permet de mettre à jour des attributs personnels de manière automatique, précise et rapide en cas de changement d'état civil. La qualité des données contenues dans les registres des utilisateurs est ainsi garantie. Grâce au fait qu'il est univoque, le NAVS permet également d'éviter les confusions administratives entre des dossiers personnels et, partant, des atteintes à la protection des données. En outre, son utilisation augmente l'efficience administrative en simplifiant les processus internes des autorités, de même que les procédures entre autorités. Depuis la mise en place des nouvelles règles en 2008, la transition vers le traitement numérique des activités administratives s'est accélérée et l'utilisation systématique du NAVS s'est beaucoup développée.

Si les dispositions actuelles de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS) prévoient une telle utilisation par les autorités, elles la soumettent à des conditions que les utilisateurs jugent malaisées à remplir. En outre, les pratiques législatives concernant l'autorisation d'une utilisation systématique du NAVS sont parfois contradictoires. Les cantons ne peuvent par ailleurs habiliter leurs autorités à utiliser le NAVS que pour l'exécution du droit cantonal. Pour ces raisons, il est de plus en plus souvent demandé que les autorités de la Confédération, des cantons et des communes soient autorisées à utiliser le NAVS comme identificateur de personnes univoque.

Contenu du projet

L'objectif du projet est de créer les conditions permettant aux autorités de la Confédération, des cantons et des communes d'utiliser systématiquement le numéro AVS en vertu d'une autorisation générale, sans avoir besoin à cette fin d'une disposition spécifique dans une loi spéciale pour chaque nouvel usage. Une plus grande transparence sera assurée du fait que les conditions d'utilisation seront les mêmes pour toutes les autorités. Par ailleurs, les organisations et les personnes qui, sans avoir le caractère d'une autorité, sont chargées par la loi de remplir des tâches administratives auront elles aussi le droit d'utiliser systématiquement le NAVS pour autant qu'une disposition le prévoie dans la loi spéciale concernée. Par contre, l'utilisation systématique du NAVS à des fins purement privées restera exclue. À l'avenir, il doit toutefois rester possible de prescrire dans les lois spéciales, à des fins particulières, des identificateurs sectoriels en lieu et place du NAVS. En ce sens, le législateur conserve sa liberté d'organisation.

Le présent projet se limite par conséquent à supprimer l'exigence actuelle d'une base juridique spécifique pour chaque utilisation systématique du NAVS en créant une autorisation d'ordre général permettant aux autorités fédérales, cantonales et communales ainsi qu'à certaines institutions d'utiliser systématiquement ce numéro. Par ailleurs, la garantie de la protection des données et de la sécurité des informations se verra accorder toute l'importance requise. Les instances habilitées à utiliser systématiquement le NAVS devront prendre des mesures techniques et organisationnelles. En premier lieu, elles auront l'obligation de protéger au mieux l'accès aux différentes bases de données afin de réduire le risque d'usage abusif au minimum. Les prescriptions de sécurité relatives à l'accès aux bases de données qui contiennent le NAVS concernent l'authentification, le transfert et le cryptage des données, leur protection contre les virus informatiques, l'utilisation de pare-feu ainsi que l'enregistrement et l'analyse des principaux processus propres aux systèmes informatiques. En obligeant les autorités qui utiliseront le NAVS à respecter ces mesures complémentaires, le projet permettra aussi d'améliorer globalement la sécurité des informations au sein de l'administration publique.

Table des matières

Message

1 Contexte

1.1 Nécessité d'agir et objectifs

1.1.1 Évolution jusqu'à ce jour

Dans l'exercice de ses activités, l'assurance-vieillesse et survivants (AVS) utilise un numéro d'assuré (numéro AVS, NAVS) depuis son instauration en 1948. À ce jour, cet identificateur de personnes sert à faciliter le traitement des informations concernant les cotisations et le calcul des prestations des assurances sociales. Au départ, le NAVS était «parlant», c'est-à-dire qu'on pouvait en déduire les premières lettres du nom de famille, la date de naissance et le sexe de la personne qu'il désignait. Cette situation s'est révélée insatisfaisante du point de vue de la protection des données. En outre, au fil du temps, il n'a plus toujours été possible d'attribuer les NAVS avec la célérité requise, ce qui a provoqué des problèmes considérables sur le plan informatique. Qui plus est, la gestion des NAVS était devenue source d'erreurs, car le numéro devait être modifié à chaque changement d'état civil. La création d'un identificateur fédéral de personnes universel (IFPU) avait donc été proposée en 2003, à l'occasion de la procédure de consultation concernant la loi sur l'harmonisation des registres[1]. Pour tenir compte des considérations liées à la protection des données, le Conseil fédéral avait proposé, lors d'une deuxième procédure de consultation à l'été 2004, d'introduire six identificateurs sectoriels de personnes (SPIN) gérés par un serveur central d'identification et de communication. Son intention était d'utiliser un identificateur de personnes univoque pour chaque secteur administratif, dont la sécurité sociale. Toutefois, les résultats de cette consultation ont montré que le projet ne parviendrait pas à convaincre la majorité des cantons. En lieu et place, la solution d'un NAVS à treize chiffres, non «parlant», a été adoptée; elle comprenait aussi des règles relatives aux conditions d'autorisation d'une utilisation systématique de ce numéro à des fins administratives en dehors de l'AVS[2].

Depuis la mise en place du nouveau NAVS en 2008, la numérisation des activités administratives a grandement progressé et l'utilisation systématique de ce numéro en dehors de l'AVS, tant au niveau de la Confédération qu'à celui des cantons, s'est beaucoup développée. Actuellement, la Centrale de compensations (CdC) compte près de 12 700 utilisateurs enregistrés. Par ailleurs, environ 60 000 fournisseurs de prestations utilisent le NAVS pour la facturation dans l'assurance-maladie obligatoire.

De nombreux acteurs estiment que les exigences posées pour l'autorisation de cette utilisation systématique doivent être assouplies. C'est ainsi qu'en janvier 2014, la Conférence des directrices et directeurs cantonaux des finances a suggéré de rendre disponible le NAVS en tant qu'identificateur de personnes afin de faire avancer les projets de cyberadministration. L'utilisation d'un identificateur univoque rendrait

1 RS **431.02**
2 RO **2007** 5259

l'administration plus efficace et améliorerait la qualité des bases de données en écartant définitivement les risques de confusion que l'on connaît aujourd'hui. Puis, lors de l'élaboration de la loi fédérale du 18 décembre 2015 sur l'échange international automatique de renseignements en matière fiscale (LEAR)[3], il a été décidé, sur la suggestion des cantons, de ne pas créer un nouveau numéro d'identification fiscale, afin d'éviter des charges administratives supplémentaires, mais d'utiliser plutôt le NAVS à cette fin. Le Préposé fédéral à la protection des données et à la transparence (PFPDT) et une partie des préposés cantonaux suivent ces développements d'un œil critique, car ils y discernent des risques en matière de protection des données.

Fort de ces constats, le Conseil fédéral a chargé en février 2017 le Département fédéral de l'intérieur (DFI) de lui soumettre une modification de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS)[4] visant à faciliter l'utilisation systématique du NAVS par les autorités fédérales, cantonales et communales dans l'accomplissement de leurs tâches légales.

L'objectif du présent projet est de créer les bases légales permettant une utilisation du NAVS qui réponde aux besoins futurs, tout en garantissant la protection des données.

1.1.2 Réglementation en vigueur

Dans le droit en vigueur, l'utilisation systématique du NAVS en dehors de l'AVS est réglée comme suit: si, aux fins de l'exécution du droit fédéral, il est nécessaire d'utiliser systématiquement le NAVS, une base légale circonstanciée peut être inscrite dans la loi fédérale concernée. La disposition légale doit cependant définir le but de l'utilisation et les utilisateurs légitimés (art. 50*d*, al. 1, et 50*e*, al. 1, LAVS). L'utilisation systématique du NAVS repose donc sur une base démocratique, puisque c'est le législateur qui en donne l'autorisation dans chaque loi spéciale concernée. Les mêmes conditions s'appliquent en principe aussi à l'utilisation du NAVS pour l'exécution du droit cantonal (art. 50*d*, al. 1, et 50*e*, al. 3, LAVS), sauf pour les quatre domaines suivants: réduction des primes dans l'assurance-maladie, aide sociale, impôts et établissements de formation. Les services cantonaux actifs dans ces domaines étant en effet déjà habilités à utiliser systématiquement le NAVS en vertu de la législation sur l'AVS (art. 50*e*, al. 2, LAVS), il n'est pas nécessaire d'édicter une disposition supplémentaire dans une loi spéciale cantonale. L'utilisation à des fins purement privées, par contre, n'est pas admise. Néanmoins, le NAVS est utilisé de manière systématique en tant que numéro d'identification fiscale dans le cadre de l'échange international automatique de renseignements en matière fiscale. Depuis l'automne 2018, il est transmis à des établissements financiers dans plus de 50 États et territoires.

Les services qui envisagent d'utiliser systématiquement le NAVS mais qui ne sont pas des assurances sociales fédérales doivent au préalable en demander l'autorisa-

3 RS **653.1**
4 RS **831.10**

tion à la CdC. Si ce droit leur est reconnu, la CdC leur ouvre l'accès à sa base de données personnelles UPI (*Unique Personal Identification*), qui sert exclusivement à l'identification de personnes. Cette base de données ne contient aucune donnée factuelle et répertorie de manière univoque toutes les personnes qui sont titulaires d'un NAVS. Outre le NAVS, elle contient également les attributs d'identité officiels des personnes physiques (nom officiel, nom de naissance, prénoms officiels, date de naissance, sexe, nationalité, pays et lieu de naissance, noms et prénoms des parents). La CdC peut garantir que les données qui y sont contenues sont à jour, complètes et univoques, car elles proviennent de sources nombreuses, les principales étant les organes d'exécution du 1er pilier de l'assurance sociale suisse ainsi que les registres des habitants de la Confédération: Infostar (registre informatisé de l'état civil), SYMIC (système d'information central sur la migration dans les domaines des étrangers et de l'asile), E-VERA (système de cyberadministration des Suisses de l'étranger) et ORDIPRO (système d'administration des fonctionnaires internationaux et des diplomates étrangers). S'ajoutent à cela les registres cantonaux et communaux des habitants, les caisses-maladie et d'autres utilisateurs du NAVS. Pour assurer la protection et la qualité des données, les services ayant un droit d'accès doivent prendre toutes les mesures techniques et organisationnelles prévues dans l'ordonnance applicable[5].

Le système actuel laisse au législateur compétent le soin de décider de l'autorisation d'utiliser systématiquement le NAVS en dehors de l'AVS. Le législateur délivre l'autorisation légale requise en se fondant sur une évaluation générale de la sécurité de l'information dans le domaine concerné.

1.1.3 Analyse des risques en exécution du postulat 17.3968 «Concept de sécurité pour les identifiants des personnes» de la Commission des affaires juridiques du Conseil national

Les explications qui suivent répondent au postulat 17.3968 «Concept de sécurité pour les identifiants des personnes», déposé le 20 octobre 2017 par la Commission des affaires juridiques du Conseil national et adopté par ce dernier en septembre 2018. Ce postulat est lié aux débats parlementaires relatifs à la modernisation du registre foncier[6] et à une analyse des risques menée en septembre 2017[7]. Il charge le Conseil fédéral de montrer dans un concept, pendant la législature en cours, de quelle manière il est possible de faire face aux risques liés à l'utilisation du NAVS à treize chiffres en tant qu'identifiant de personne unique, et de quelle manière la

5 Ordonnance du DFI du 7 novembre 2007 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 (RS **831.101.4**).

6 www.parlement.ch > 14.034 «CC. Enregistrement de l'état civil et registre foncier».

7 David Basin, «Risk Analysis on Different Usages of the Swiss AHV Number», EPF Zurich, Institut für Informationssicherheit, Zurich, 2017; cf. www.leprepose.ch > Protection des données > Statistique, registre et recherche > Numéro AVS (texte en anglais, résumé en français).

protection des données dans le cadre de l'utilisation de numéros d'identification de personnes par les cantons, les communes et des tiers peut être améliorée, en prenant pour cela en considération l'avis du PFPDT.

Remarques préliminaires

Il arrive régulièrement que la nature et la fonction des identificateurs de personnes soient peu claires. De nombreuses hypothèses, pas toujours exactes, circulent en outre quant aux risques posés par l'utilisation systématique d'identificateurs de personnes en général, et du NAVS en particulier. Dans ce contexte, le postulat exige que la situation soit clarifiée. Des identificateurs modernes tels que le NAVS ne sont pas parlants; ils ne permettent pas d'accéder à des systèmes informatiques, ni de s'authentifier sur Internet (ce n'est pas un identifiant de type e-ID). Le seul risque réel pour la protection des données que présente l'utilisation systématique d'identificateurs univoques est que ces derniers peuvent permettre de créer des profils de personnalité plus précis que ceux pouvant être élaborés à partir des données publiques ou connues de la personne qui les réalise. Par profil de la personnalité, on entend un assemblage de données qui permet d'apprécier des aspects essentiels de la personnalité d'une personne physique. La mesure dans laquelle ce risque existe est exposée ci-après. Les approches permettant de le réduire dans une mesure raisonnable et réalisable sont également expliquées. La mission du législateur est en revanche d'évaluer si et, le cas échéant, dans quelles conditions les avantages de l'utilisation systématique du NAVS l'emportent sur le risque résiduel.

Définition et fonction des identificateurs de personnes

Un identificateur de personnes sert à associer correctement les informations au sein d'une collection de données personnelles. À la différence du nom ou du prénom, qui peuvent parfois être identiques et créer la confusion, un identificateur unique permet d'associer de manière univoque des ensembles de données à des personnes. Il empêche toute confusion entre les dossiers, et la qualité des données dans les registres s'en trouve augmentée.

Tout comme d'autres identificateurs de personnes de la Confédération, le NAVS a pour seule fonction d'associer à la personne concernée un jeu de données personnelles au sein d'une collection de données. Il est utilisé à des fins exclusivement administratives. Toute personne physique se voit attribuer un NAVS peu après sa naissance sur territoire suisse, ou après justification de domicile ou de résidence habituelle en Suisse. Il s'agit d'un numéro d'identification de la personne univoque, non modifiable et que la personne conserve toute sa vie.

Il n'est pas totalement exclu qu'un même numéro puisse être attribué à plusieurs personnes, mais les mécanismes de contrôle actuels sont si développés que de telles erreurs restent rares et qu'elles peuvent rapidement être découvertes et corrigées. La CdC signale les NAVS annulés ou désactivés aux instances habilitées à les utiliser afin que celles-ci puissent actualiser en conséquence leurs bases de données.

Sous l'angle des identificateurs de personnes utilisés, les registres régis par le droit fédéral s'avèrent disparates. En dehors des assurances sociales aussi, il existe des registres de personnes qui utilisent uniquement le NAVS en tant qu'identificateur de personnes, comme le registre dosimétrique central des personnes professionnelle-

ment exposées aux radiations[8]. D'autres registres centraux de la Confédération, comme SYMIC, E-VERA ou ORDIPRO, utilisent un identificateur de personnes propre à leur système en plus du NAVS. Il en va de même pour le registre des professions médicales[9] et le registre des professions de la santé[10]. Le droit fédéral prévoit également que le NAVS permet aux autorités cantonales du registre du commerce d'identifier les personnes physiques. En outre, un numéro spécifique au registre est attribué aux personnes enregistrées dans la base de données centrale des personnes[11]. Le numéro d'identification univoque utilisé pour le dossier électronique du patient (DEP) est un numéro spécifique délivré et géré par la CdC; il y est lié au NAVS[12].

Le numéro d'identification des entreprises (IDE) n'est pas un identificateur de personnes au sens strict, d'autant qu'il peut aussi être attribué à des communautés de personnes sans personnalité juridique[13]. Il en va de même pour le registre des entreprises et des établissements (REE), qui contient les données relatives aux entreprises et aux établissements de droit public et de droit privé ayant leur siège en Suisse[14].

Le NAVS ne permet de tirer aucune conclusion sur les attributs d'une personne

Seuls les identificateurs de personnes qui sont parlants permettent de connaître des attributs de leur titulaire. Un identificateur de personnes est donc dit parlant lorsqu'il contient des informations codées sur l'état civil, l'âge, le sexe ou d'autres attributs personnels de son titulaire, ce qui peut entraîner la révélation non souhaitée de données personnelles. En outre, des difficultés surgissent dès qu'il y a changement de données personnelles (par ex. du nom de famille). En revanche, un identificateur généré aléatoirement ou sous forme de numéro de série séquentiel ne contient pas d'information codée sur son titulaire et est donc non parlant[15]. Les identificateurs usuels au niveau fédéral sont exclusivement des numéros non parlants[16]. Le NAVS ne contient aucune information relative à son titulaire et ne permet donc de tirer aucune conclusion quant à ses attributs personnels, à la différence du numéro à onze chiffres qu'a remplacé le numéro à treize chiffres utilisé aujourd'hui (cf. 1.1.1). Afin que leur origine soit identifiable, tous les NAVS commencent par le préfixe «756»,

8 Art. 72 à 76 de l'ordonnance du 26 avril 2017 sur la radioprotection (RS **814.501**).
9 Art. 51, al. 4bis, de la loi du 23 juin 2006 sur les professions médicales (LPMéd; RS **811.11**).
10 Art. 24, al. 3, de la loi fédérale du 30 septembre 2016 sur les professions de la santé (LPSAN; FF **2016** 7383); pas encore entré en vigueur
11 Art. 928*c*, al. 1 et 3, du code des obligations (CO); FF **2017** 2261; pas encore entré en vigueur.
12 Art. 4 et 5, al. 1, de la loi fédérale du 19 juin 2015 sur le dossier électronique du patient (LDEP; RS **816.1**).
13 Entités IDE au sens de l'art. 3, al. 1, let. c, de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises (LIDE; RS **431.03**).
14 Art. 3, al. 1, de l'ordonnance du 30 juin 1993 sur le Registre des entreprises et des établissements (OREE; RS **431.903**).
15 Art. 25, al. 1, 2^{e} phrase, de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (RS **235.11**): «Est un identifiant non signifiant tout ensemble de caractères attribué de manière biunivoque à chaque personne enregistrée dans un fichier et qui ne livre par lui-même aucune information sur la personne.».
16 Au sens de l'art. 3, let. e, de la loi du 23 juin 2006 sur l'harmonisation de registres (LHR; RS **431.02**), un identificateur est un numéro immuable ne permettant aucune déduction sur la personne ou la chose à laquelle il a été attribué.

code correspondant à la Suisse selon la norme ISO 3166. Les neuf chiffres suivants sont une combinaison aléatoire unique parmi les suites de chiffres n'ayant pas encore été attribuées. Le treizième et dernier chiffre est une clé de contrôle.

Le NAVS n'est pas un code d'authentification

Le processus d'authentification garantit que la personne est bien celle qu'elle prétend être. En cas d'authentification au moyen d'un mot de passe, le système demande à l'utilisateur de prouver la véracité de son affirmation en donnant une information dont lui seul a connaissance (authentification basée sur la connaissance). La mention du NAVS n'est pas une option possible dans une telle procédure.

Les applications bureautiques usuelles des administrations publiques utilisent en général une double authentification (par ex. une carte à puce de la Confédération en combinaison avec un mot de passe personnel) pour contrôler les droits d'accès. Pour l'utilisation d'applications spécialisées, en particulier de celles qui donnent accès à des données personnelles, des informations supplémentaires spécifiques à l'application sont requises (code d'utilisateur et mot de passe). Le NAVS n'est pas un sésame qui ouvre l'accès à des systèmes informatiques. La connaissance d'un identificateur de personnes comme le NAVS ne permet donc pas de pénétrer un système informatique auquel on n'a normalement pas accès. L'utilisation systématique d'identificateurs de personnes dans une collection de données n'en accroît donc pas la vulnérabilité. Le NAVS n'est pas non plus une preuve d'identité (numérique), par exemple sur Internet. Il est ainsi impossible d'obtenir des prestations étatiques sur simple indication du NAVS. La connaissance de son propre NAVS ou de celui d'une autre personne ne permet en aucun cas d'en tirer un quelconque bénéfice financier ou immatériel.

Le NAVS ne confère pas un accès étendu à d'autres bases de données

Les autorités qui sont habilitées à utiliser systématiquement le NAVS peuvent associer à ce dernier les attributs usuels de la personne correspondante, comme son nom ou sa date de naissance. Les données factuelles d'une personne sont alors liées en premier lieu à ce numéro dans la base de données. Afin de garantir qu'elle utilise le bon numéro ou que les autres attributs sont corrects, l'autorité a accès à la base de données UPI. Cela ne lui donne toutefois pas accès aux autres registres, en particulier au registre central des assurés et au registre central des prestations de la CdC, ni aux registres de données factuelles gérés par d'autres autorités. L'habilitation à utiliser le NAVS n'autorise en aucun cas une autorité à procéder à des appariements de données (cf. ci-après).

Appariements de données à l'aide d'identificateurs de personnes et profils de la personnalité

L'appariement des données contenues dans différents systèmes au sujet d'une même personne peut permettre d'en tirer un profil de la personnalité. Un tel profil contient non seulement les attributs d'identité de base d'une personne, comme son nom, son prénom, sa date de naissance mais aussi, en fonction des bases de données utilisées, d'autres informations personnelles, relatives par exemple à la santé ou à la fiscalité. Les appariements illicites et de ce fait inacceptables sont techniquement réalisables

lorsqu'une personne arrive à infiltrer plusieurs bases de données. L'utilisation des mêmes identificateurs de personnes univoques par plusieurs bases de données améliore la précision des résultats et facilite l'appariement de données, quoique dans une faible mesure. Toutefois, des appariements peuvent aussi être réalisés sans identificateurs de personnes, par exemple à l'aide de quasi-identifiants comme le nom et le prénom. L'utilisation d'identificateurs de personnes ne les rend pas plus faciles.

Les profils de la personnalité peuvent être utilisés à des fins commerciales. Selon leur niveau de précision, en faire commerce peut rapporter gros. Les acheteurs de profils de la personnalité ont généralement pour but d'élargir leur clientèle ou d'en savoir plus sur leurs clients. Les agences d'évaluation du crédit, qui évaluent la solvabilité des personnes en se fondant sur des bases de données, s'intéressent elles aussi aux profils de la personnalité. Il convient de faire preuve de prudence lorsque des acteurs étatiques réalisent des profils de la personnalité à partir de données numériques. S'ils le font dans le cadre de processus régis par la loi et légitimés démocratiquement, par exemple à des fins statistiques ou pour pouvoir répondre à des questions scientifiques claires, il n'y a rien à y redire. Afin d'éviter d'éventuels problèmes, les autorités sont autorisées à produire des profils de la personnalité (par ex. à des fins statistiques) uniquement lorsqu'une base légale le permet expressément.

Les profils de la personnalité peuvent également être utilisés abusivement en vue de procéder à un vol de données ou à une usurpation d'identité. Ce qu'on appelle communément vol de données fait référence à l'obtention non autorisée d'informations. Lorsque les informations concernent une personne donnée et sont utilisées abusivement par la suite, on parle d'usurpation d'identité. Cela consiste à se faire passer pour une autre personne afin d'obtenir des prestations auxquelles on n'a pas droit; en parallèle, cela rend difficile voire impossible d'établir l'identité effective de l'usurpateur. Les données personnelles qui, dans leur ensemble, constituent une identité sont par exemple le nom et le prénom, la date de naissance, les numéros des documents d'identité, des comptes bancaires ou des cartes de crédit ainsi que les mots de passe, les codes d'accès et les pseudonymes. Plus l'usurpateur dispose d'informations, plus l'usurpation d'identité est facile. Elle est souvent réalisée dans le but de porter atteinte à la réputation de quelqu'un ou de se procurer un avantage financier illicite. Réussir à usurper une identité dépend entre autres du choix de la personne visée en matière d'authentification (document officiel ou identification électronique e-iD). La connaissance d'un identificateur de personnes ne permet pas à elle seule de voler des données.

Probabilité de survenance et ampleur potentielle du dommage

Tous les registres officiels de personnes doivent contenir les attributs d'identité (par ex. nom, prénom et date de naissance) des personnes enregistrées. Il s'agit de ce qu'on appelle des quasi-identifiants. Si une personne (ou un logiciel) arrive à s'introduire sans autorisation dans plusieurs bases de données, elle peut déjà apparier les données personnelles qui s'y trouvent à l'aide des quasi-identifiants, même si ces bases de données n'utilisent pas d'identificateur de personnes à proprement parler, comme le NAVS. Le degré de fiabilité change toutefois en fonction des attributs d'identité contenus dans les bases de données: s'il s'agit seulement du nom

et du prénom, la précision des appariements est de 75,89 %. Par contre, si ce sont le nom, le prénom et la date de naissance, la précision atteint 99,98 %[17]. Si les données sont appariées à l'aide non pas des attributs d'identité mais d'un identificateur univoque comme le NAVS, la précision est de 100 % et donc de 0,02 % supérieure à celle d'un appariement basé sur le nom, le prénom et la date de naissance. En l'occurrence, il s'agit (seulement) du risque découlant (exclusivement) de l'enregistrement, dans un registre de personnes, du NAVS (soit d'un identificateur de personnes univoque) en plus des quasi-identifiants déjà utilisés.

La question se pose donc de savoir si la seule perspective d'une augmentation de 0,02 % de la précision peut inciter des personnes à s'introduire ou tenter de s'introduire sans autorisation dans des bases de données pour produire des profils de la personnalité illicites qu'elles n'auraient pas pu réaliser autrement, ou pour améliorer ou compléter des profils de la personnalité déjà créés. Autrement dit, faut-il supposer que l'amélioration de 0,02 % de la précision constituerait une incitation décisive pour ces personnes ? Il est impossible d'évaluer de manière définitive si cela les pousserait effectivement à infiltrer ou à tenter d'infiltrer illégalement des systèmes d'information. Les bases de données suisses contenant des données personnelles présentent déjà une précision élevée même sans utiliser d'identificateur de personnes comme le NAVS et pourraient s'avérer intéressantes à cet égard. En tout état de cause, le fait qu'une personne non autorisée arrive à s'introduire dans un système dépend en premier lieu de l'état des mesures de sécurité des informations. C'est donc avant tout l'effort à fournir pour infiltrer un système qui est déterminant. En d'autres termes, plus un système est sécurisé, moins une précision élevée constitue une incitation à s'y introduire. Si la sécurité des données est garantie, le vol de données ou l'usurpation d'identité et la création illicite de profils de la personnalité sont exclus. Par contre, lorsque cette sécurité n'est pas garantie, le risque s'accroît. Le fait qu'un identificateur de personnes figure également parmi les données enregistrées ne change rien sous l'aspect de la vulnérabilité d'un système informatique.

L'appréciation d'un risque consiste à confronter la probabilité de survenance d'un événement avec le degré de gravité du dommage qui en résulterait. Il est impossible de prévoir avec exactitude si la légère extension de l'utilisation systématique du NAVS facilitera la création illicite de profils de la personnalité sur cette base. La probabilité est toutefois très faible, car il reste possible de créer des profils de la personnalité très précis ou de voler des données même sans NAVS, en infiltrant plusieurs bases de données. Il est également difficile d'évaluer de manière globale la gravité des possibles atteintes à la personnalité que la création illicite de profils de la personnalité pourrait avoir. Cela dépend du type de données personnelles pouvant être reliées concrètement. L'appariement de données facilement accessibles (comme l'adresse et le sexe) est nettement plus anodin que, par exemple, l'appariement illicite de données sur la santé avec les éventuels antécédents pénaux. Si les prescriptions relatives à la sécurité informatique sont respectées strictement, il est toutefois extrêmement peu probable, dans un cas comme dans l'autre, que ce risque se réalise.

17 Cf. Basin, op. cit., ch. 2.2.3, p. 11.

Mesures

Mesures contre les intrusions illicites de personnes non autorisées

La mise en place de la sécurité informatique n'est pas une mesure isolée, mais un processus perpétuel qui nécessite l'observation et l'adaptation constantes de divers facteurs. Afin d'éviter que des indésirables (pirates informatiques) infiltrent des systèmes informatiques, les espionnent et apparient les données qui y sont contenues, il faut tenir en permanence à jour les processus et les procédures de sécurité. Le contrôle doit être permanent et d'autant plus minutieux lorsque le système concerné contient des données personnelles. Il faut tout particulièrement veiller à ce que les bases de données soient protégées contre les consultations et les manipulations non autorisées. Les bases de données et les applications spécialisées exploitées par la Confédération présentent dans l'ensemble un niveau de sécurité relativement élevé. C'est également le cas de nombreux systèmes informatiques des cantons et des communes. Il existe néanmoins, en dehors de l'administration fédérale, plusieurs systèmes qui ne satisfont pas entièrement aux normes de sécurité actuelles. Cette situation doit être corrigée à l'aide de mesures de sécurité. Un niveau de sécurité suffisant ne peut être atteint que si des prescriptions touchant l'organisation, le personnel, l'infrastructure et la technique sont respectées.

Concrètement, cela signifie d'abord que les responsabilités en matière de sécurité informatique doivent être réglées. Elles doivent l'être de façon compréhensible pour toutes les tâches essentielles, en particulier dans le processus de sécurité de l'information, afin de délimiter les tâches respectives, mais aussi d'éviter toute lacune en matière de responsabilité. Les collaborateurs qui ont à faire avec des moyens informatiques doivent être formés aux mesures de sécurité dans l'utilisation de cette infrastructure. Les directives et instructions en matière de sécurité devront être consignées par écrit. Il faudra vérifier régulièrement les risques dans le domaine de la sécurité de l'information, et établir un concept de sécurité de l'information et de protection des données (SIPD). Pour ce qui est de la sécurité physique, il importe, d'une part, de sécuriser l'accès aux moyens informatiques et aux unités de mémoire. D'autre part, avant leur réparation, élimination ou destruction, il faut s'assurer que ceux-ci ne contiennent plus ni NAVS ni autres données personnelles, et que ces données ne puissent pas être reconstituées.

Il importe par ailleurs de réduire au minimum, sur le plan technique, les risques d'accès non autorisé. Cela inclut de mettre en place une procédure d'authentification appropriée et de prendre des mesures de sécurité informatique (logiciel antivirus, système pare-feu). Les logiciels devront correspondre à l'état de la technique et faire régulièrement l'objet de mises à jour de sécurité et d'élimination des erreurs (patches de débogage). Pour les réseaux mobiles, les données devront être cryptées au moyen de procédures conformes aux dernières possibilités techniques. L'analyse régulière et systématique des fichiers journaux des ordinateurs permettra d'identifier les irrégularités ou les dysfonctionnements des systèmes informatiques qui sont dus à des programmes défectueux, à l'absence d'un programme ou à des failles de sécurité. Les incidents de sécurité devront être traités rapidement et efficacement afin d'empêcher ou de limiter l'espionnage, la manipulation ou la destruction de données. Par incident de sécurité, on entend un événement non souhaité qui a un impact sur la sécurité de l'information et qui peut entraîner par la suite des dom-

mages importants. Une procédure préétablie et éprouvée dans ce domaine pourra ainsi contribuer à réduire les temps de réaction. Le traitement des incidents de sécurité devra donc être pensé et testé en amont.

Mesures contre le traitement illicite de données par l'État

Le principe de proportionnalité du traitement des données prévoit qu'une autorité peut, par principe, accéder uniquement aux données pour lesquelles elle est directement compétente. Il faut en outre veiller à ce qu'elle ne collecte que les données dont elle a effectivement besoin. Les processus d'échange de données ne doivent en outre pas pouvoir être étendus à volonté. Ces exigences, qui répondent aux principes fondamentaux du droit de la protection des données, doivent être prises en compte dans la législation relative aux registres concernés.

La mise en réseau des systèmes d'information des autorités s'accroît toutefois continuellement. Lorsque les bases légales l'autorisent, les autorités échangent régulièrement des informations entre elles. D'un côté, les systèmes d'information de diverses autorités sont reliés entre eux par des interfaces, et de l'autre, des autorités reçoivent des droits d'accès, par des procédures d'appel, aux bases de données d'autres autorités. La procédure d'appel est une procédure automatisée au cours de laquelle une personne peut se procurer elle-même l'information recherchée, sans que l'administration le sache ou ait besoin de le savoir. Il arrive aussi régulièrement que le traitement des données soit concentré grâce au regroupement de plusieurs systèmes informatiques, ce qui présente l'avantage de ne pas devoir saisir séparément les données de base comme les informations personnelles dans chaque système d'information; les droits d'accès des services rattachés ne sont ainsi pas étendus à d'autres données. En outre, la comparaison et la transmission de données ont de plus en plus lieu par voie électronique. La possibilité pour les autorités d'utiliser systématiquement un identificateur de personnes à usage général dans leurs registres crée une condition technique permettant aux échanges de données prévus par la loi d'avoir lieu sous forme automatisée et donc efficace.

Des mesures préventives devront être prises afin que les autorités ne puissent pas créer illégalement des profils de la personnalité. Il faudra donc veiller de manière générale à ce que la transmission et la comparaison de données ne puissent être automatisées que lorsque c'est nécessaire. Il incombera en outre au législateur de prendre les décisions requises à ce sujet. Cela nécessitera donc une base légale prévoyant explicitement que l'échange de données peut se faire au moyen du NAVS, et donc par voie électronique[18]. Une autre possibilité consistera à surveiller systématiquement les interfaces des systèmes informatiques au sein de l'administration en réalisant des analyses de risques périodiques.

Des identificateurs sectoriels de personnes pour une meilleure sécurité de l'information ?

Dans son rapport mentionné précédemment[19], l'expert rappelle qu'aucun système ne peut être entièrement protégé contre les attaques. Il expose en outre divers moyens

18 Cf. art. 32*a*bis, al. 2, de la loi du 20 juin 1997 sur les armes (RS **514.54**).
19 Cf. Basin, op. cit.

permettant de contrer les multiples possibilités d'apparier (au moyen de quasi-identifiants ou du NAVS) les données personnelles contenues dans les bases de données. Si l'on entend éradiquer les problèmes liés à la protection des données, l'expert conseille donc de revoir la conception de l'ensemble des bases de données. Les données personnelles et les données factuelles devraient être enregistrées dans des bases de données séparées. De plus, les données personnelles devraient y être exemptes de redondances. Il y a redondance dans les informations lorsque des données ayant un contenu informatif identique figurent plusieurs fois. Des attributs tels que le nom, le prénom ou le NAVS d'une personne devraient donc n'être enregistrés que dans une seule base de données. L'appariement des données personnelles avec les données factuelles ne devrait être possible qu'au moyen de «tables de liens» (*linkage tables*) spéciales, tenues secrètes. La seule mise en place d'identificateurs spécifiques aux secteurs, sans que les modifications exposées concernant l'architecture du système aient été apportées, ne serait par contre pas judicieuse.

Amélioration de la protection des données dans l'utilisation des numéros d'identification de personnes par les cantons, les communes et les tiers

Les arguments avancés au sujet des identificateurs de personnes de la Confédération en général et du NAVS en particulier valent aussi, par analogie, pour les identificateurs de personnes des cantons. Il incombera toutefois toujours à ces derniers de régler eux-mêmes l'attribution et l'utilisation systématique de ces identificateurs. Lors de l'édiction des prescriptions relatives à la protection des données, ils devront tenir compte du droit constitutionnel à la protection de la sphère privée visé à l'art. 13, al. 2, de la Constitution (Cst.)[20]. En vertu de cette disposition, les cantons sont tenus de prendre toutes les mesures nécessaires pour protéger les citoyens contre un emploi abusif des données qui les concernent.

1.1.4 Digression: utilisation du numéro de sécurité sociale américain

L'utilisation étendue du numéro de sécurité sociale américain est un point souvent abordé. Aux États-Unis, les autorités et même les particuliers ont largement recours au numéro de sécurité sociale (*social security number*, SSN). Il y a plusieurs explications à cela. D'une part, la gestion officielle des registres et des documents d'identité y est du ressort des États; elle est donc réglée différemment dans chacun d'entre eux. En même temps, cette structure reflète typiquement la conception de la répartition des compétences et des tâches dans ce pays. Là-bas, il serait impensable d'instaurer un registre centralisé répertoriant les données relatives à l'identité et à l'état civil de toute la population résidente. Un tel système, qui est la norme dans de nombreux pays européens, serait perçu comme une tentative de surveillance excessive par l'État et serait largement rejeté. Dans ces circonstances, la carte de sécurité sociale américaine (*social security card*) sur laquelle est inscrit le SSN constitue le seul moyen d'identification uniforme à l'échelle du pays, puisqu'en principe toute la population dispose d'un SSN. De ce fait, la carte de sécurité sociale ou le SSN sont

20 RS **101**

souvent utilisés comme moyen d'identification, mais aussi à des fins d'authentification.

D'autre part, aux États-Unis, même des particuliers sont habilités à utiliser systématiquement le SSN. Les trois principales «bases de données de solvabilité» (ou agences d'évaluation du crédit), notamment, travaillent avec le SSN. Il en va de même pour les sociétés de carte de crédit, les banques, les sociétés de crédit-bail et les entreprises semblables, auxquelles les agences d'évaluation du crédit demandent régulièrement des informations. Le SSN leur permet de se servir de ces informations pour créer des profils de la personnalité relatifs à la situation financière de personnes données en vue d'évaluer leur solvabilité. Le risque d'usurpation d'identité en lien avec le SSN doit donc être étudié au regard de ce contexte. L'usurpation d'identité (de préférence d'une identité présentant une bonne solvabilité) en vue d'obtenir un crédit nécessite donc notamment de connaître le SSN de la victime.

Il est judicieux de tenir compte de ce point pour ce qui est du projet d'utilisation étendue du NAVS. Il faut souligner que la réglementation prévue se distingue de la situation américaine: même à l'avenir, l'utilisation du NAVS par les particuliers sera exclue en Suisse. En outre, contrairement aux États-Unis, la Suisse dispose d'un service de gestion des registres et des documents d'identité uniforme au niveau national. Cela permet de garantir que toute authentification ne puisse se faire qu'au moyen d'une pièce d'identité officielle, même à l'avenir. Il n'y a donc pas lieu de craindre que des vols de données ou des usurpations d'identité résultent de l'utilisation élargie du NAVS par les autorités de la Confédération, des cantons et des communes.

1.2 Solution retenue et autres possibilités examinées

1.2.1 Solution retenue: utilisation systématique du NAVS par toutes les autorités

L'utilisation systématique du NAVS dans une collection de données personnelles permet une identification univoque et une meilleure qualité des données. Il est possible de parer aux éventuels risques que cela implique au moyen de mesures supportables. L'autorisation générale donnée aux autorités fédérales, cantonales et communales d'utiliser systématiquement le NAVS s'avère une solution équilibrée tant sur le plan de la pertinence et de la faisabilité que de la proportionnalité. Il faut en particulier tenir compte des points suivants:

Prévention des erreurs administratives coûteuses

L'accroissement de la population et celui des tâches des administrations publiques se traduisent par une augmentation du volume des données et du nombre de mutations. À cela s'ajoute un nombre croissant de noms complexes (par ex. doubles noms, noms écrits avec des caractères spéciaux ou dans une écriture non latine nécessitant une transcription). Un traitement manuel prend beaucoup de temps et peut être source d'erreurs. Le recours à un identificateur de personnes sous forme de séquence de chiffres contribue notablement à résoudre ces problèmes. Cela vaut en particulier pour l'utilisation du NAVS, d'autant que les fichiers de la base de données UPI,

entretenus avec soin, sont très fiables. Une notification appropriée du SYMIC et d'Infostar permet d'actualiser en permanence les attributs personnels enregistrés dans la base de données UPI. La qualité élevée des données de cette dernière garantit donc qu'une personne puisse être identifiée correctement. Par conséquent, l'utilisation systématique du NAVS dans le cadre du traitement des données contribuera à éviter toute confusion de données personnelles.

Amélioration de l'efficacité grâce à l'échange de données automatisé entre les autorités

L'utilisation systématique d'un identificateur de personnes univoque permettra aux autorités d'échanger des données en continu. Par «en continu», on entend sans changer de support d'information dans un même processus de traitement d'information, donc sans interrompre le processus parce qu'il faudrait renvoyer les données dans un autre format que celui dans lequel elles ont été reçues. C'est le cas, par exemple, lorsque des informations disponibles sur un support électronique sont imprimées et traitées sur papier, puis réintroduites à la main dans un autre système informatique. Lorsque le législateur l'autorisera expressément, la communication de données pourra avoir lieu de manière automatisée à l'aide du NAVS, ce qui simplifiera les processus internes et transversaux entre les autorités et produira un gain d'efficience. Cela permettra donc un usage efficace et économe des fonds publics, comme l'exigent les art. 43*a*, al. 5, Cst. et 12, al. 4, 2e phrase, de la loi du 7 octobre 2005 sur les finances[21]. Les fonds publics seront également épargnés, puisque le travail législatif d'adaptation des lois spéciales aux niveaux fédéral, cantonal et communal ne sera plus nécessaire.

Les appariements de données prévus par le législateur et par conséquent licites, par exemple à des fins statistiques[22], produisent également des résultats plus précis quand ils peuvent être effectués au moyen d'un identificateur de personnes univoque.

Prévention de la confusion

Pour les simples citoyens – en particulier ceux qui portent un nom très répandu –, l'utilisation systématique du NAVS apporte également une plus-value: toute personne dont les données personnelles sont recueillies a droit à ce que les processus administratifs fondés sur ces données se déroulent sans aboutir à des confusions avec d'autres personnes enregistrées. Pour les personnes concernées, de telles confusions peuvent entraîner des désagréments considérables. Les erreurs de ce type résultent en règle générale d'imprécisions dans la tenue des registres, de fautes d'orthographe ou du fait qu'un nom ou une combinaison de noms sont très répandus. Ainsi, il n'y a pas moins de 950 Peter Müller sur les 2 330 700 numéros de téléphone privés enregistrés dans l'annuaire officiel suisse. Si les personnes sont enregistrées dans une base de données avec un identificateur de personnes univoque, tout

21 RS **611.0**

22 Les appariements à des fins statistiques sont réalisés en vertu de l'art. 14*a* de la loi du 9 octobre 1992 sur la statistique fédérale (RS **431.01**), de l'art. 14 de l'ordonnance du 30 juin 1993 sur les relevés statistiques (RS **431.012.1**) et de l'ordonnance du 17 décembre 2013 sur l'appariement de données (RS **431.012.13**).

risque de confusion est écarté. Cette amélioration de la qualité des données dans les registres d'utilisateurs contribuera à garantir l'exactitude des données, ce qui répond à une exigence importante de la protection de la personnalité dans l'utilisation des données personnelles (cf. 1.1.3).

Maintien de la possibilité de numéros sectoriels

Le présent projet maintient la possibilité d'interdire, dans une loi spéciale, l'utilisation systématique du NAVS pour certains registres, afin de pouvoir exclure tout risque résiduel concernant la création de profils de la personnalité dans les domaines traitant des données particulièrement sensibles.

Mesures d'accompagnement et analyses régulières des risques

Le respect des mesures d'accompagnement exige des utilisateurs du NAVS qu'ils tiennent continuellement à jour leurs systèmes d'information. Le présent projet contribue ainsi à l'amélioration générale de la sécurité de l'information dans l'administration publique. Si les analyses des risques sont réalisées régulièrement et si les mesures d'accompagnement sont mises en œuvre avec rigueur, l'utilisation systématique du NAVS ne risque ni de menacer la protection des données ni de rendre toutes les données personnelles transparentes.

1.2.2 Autres possibilités examinées

Procédure d'autorisation

Dans un système soumis à autorisation, la compétence d'utiliser systématiquement le NAVS serait accordée non pas au législateur, mais à une autorité compétente par voie de décision. Cette autorité devrait examiner dans chaque cas si l'entité requérante est en mesure d'assurer la protection des données et la sécurité de l'information lorsqu'il utilise le NAVS. Le requérant devrait notamment prouver qu'il est en mesure de prendre toutes les mesures techniques et organisationnelles requises. L'autorité qui accorde l'autorisation devrait en outre vérifier au moyen de contrôles périodiques procédant par échantillonnage auprès des titulaires d'autorisation si ces derniers remplissent toujours les conditions d'octroi et s'ils respectent l'obligation de diligence et celle de collaborer. Un tel système ne pourrait toutefois être mis en place qu'au prix d'une augmentation des charges administratives et en particulier de frais élevés sans commune mesure avec le bénéfice supplémentaire qui pourrait en résulter, d'autant que les systèmes informatiques sont soumis par nature à des changements constants et que l'octroi de l'autorisation ne pourrait se faire que sur la base de la situation à ce moment précis. Étant donné qu'il est reconnu que les autorités fédérales, cantonales et communales font preuve d'un grand respect de la loi, il convient d'éviter de mettre en place des mécanismes de contrôle et de surveillance dispendieux, et de miser plutôt sur le principe de l'autocontrôle.

Numéros sectoriels

Un système fonctionnant avec des identificateurs sectoriels a également été examiné. Dans un tel système, plusieurs identifiants seraient attribués à chaque personne physique à enregistrer. Chacun de ces identifiants ne pourrait être utilisé que dans le domaine d'activité du secteur administratif concerné, par exemple le secteur fiscal ou celui des assurances sociales. Pour qu'une communication électronique efficace puisse tout de même être établie entre deux services administratifs relevant de secteurs différents, un serveur central d'identification et de communication serait indispensable. Dans la structure actuelle de l'administration, de tels secteurs n'existent toutefois pas. Il faudrait donc commencer par les créer. À l'occasion de la consultation de 2004 sur le projet de loi fédérale sur les identificateurs sectoriels de personne, la plupart des cantons et des organisations ont estimé qu'en ce qui concerne la cyberadministration, une sectorialisation serait trop complexe et trop coûteuse, qu'elle serait en plus source d'erreurs et qu'elle ne constituait par conséquent pas une solution réalisable.

Du point de vue actuel, l'introduction généralisée d'identificateurs de personnes sectoriels ou autres ne serait pas souhaitable pour de nombreuses autorités fédérales, cantonales et communales, car elle serait trop coûteuse et ne diminuerait en rien les risques existants. Cela constituerait même en partie une régression, d'autant que des dispositions ont déjà été édictées et que des investissements ont déjà été réalisés dans la conviction que la réglementation actuelle (avec le NAVS comme identificateur de personnes univoque pour les autorités) serait maintenue. Dans ces circonstances, la mise en place d'un vaste système fonctionnant avec des identificateurs sectoriels de personne n'est pas souhaitable. Mais si, dans un domaine précis, l'utilisation d'un identificateur de personnes particulier était souhaitée, cela resterait possible avec le projet proposé.

1.3 Relation avec le programme de la législature et avec les stratégies nationales du Conseil fédéral

1.3.1 Relation avec le programme de la législature

Le présent projet n'est annoncé ni dans le message du 27 janvier 2016 sur le programme de la législature 2015 à 2019[23] ni dans l'arrêté fédéral du 14 juin 2016 sur le programme de la législature 2015 à 2019[24]. Cependant, il contribue à la mise en œuvre de la Stratégie suisse de cyberadministration (cf. 4.2), projet mentionné, quant à lui, dans le programme de la législature 2015 à 2019.

23 FF **2016** 981
24 FF **2016** 4999

1.3.2 Relation avec les stratégies du Conseil fédéral

La Stratégie suisse de cyberadministration[25] adoptée par le Conseil fédéral vise à fournir de meilleures prestations aux acteurs économiques et à la population, et à les faire profiter d'une administration plus efficace. L'instrument de mise en œuvre de la stratégie actuelle est le Plan stratégique 2017-2019[26]. Celui-ci comporte onze objectifs opérationnels, le nº 7 étant le suivant: «L'attribution des données à une personne déterminée dans l'échange électronique entre systèmes d'information est garantie d'ici à 2019». Il est ensuite précisé qu'il n'a pas encore été possible de créer un identifiant personnel univoque utilisable dans tous les domaines spécialisés et à tous les échelons de l'État, bien que l'on en ressente fortement le besoin. Le présent projet contribue donc à la mise en œuvre de la Stratégie suisse de cyberadministration.

Le plan stratégique susmentionné prévoit aussi l'introduction d'un moyen d'identification électronique reconnu par l'État (e-ID; objectif opérationnel nº 5). Des identités certaines constituent la base de la sécurité juridique. Le projet de loi fédérale sur les services d'identification électronique (LSIE) adopté par le Conseil fédéral[27] a pour objectif de favoriser la sécurité de l'échange électronique de données entre les particuliers et les autorités, ainsi qu'entre particuliers. Afin que des processus commerciaux même relativement complexes puissent se dérouler en ligne, les partenaires contractuels doivent pouvoir se fier à l'identité de leur interlocuteur. La création d'unités d'identification reconnues pour les personnes physiques permettra de répondre à ce besoin. Le numéro d'enregistrement e-ID, indépendant de l'AVS, servira à faire le lien entre la personne et l'e-ID émis.

Le numéro d'enregistrement e-ID est basé sur une répartition des tâches entre l'État et les particuliers: la Confédération n'édite aucun e-ID propre, mais peut reconnaître officiellement des e-ID de fournisseurs privés (comme le SuisseID de la Poste), s'ils remplissent les exigences légales. Cette reconnaissance permet aux fournisseurs de services d'identification (*Identity Provider*, IdP) d'utiliser des données d'identification personnelle introduites et confirmées par l'État pour la fourniture de leurs services. Il sera donc permis aux IdP d'utiliser systématiquement le NAVS, mais exclusivement dans ce but précis. En outre, les IdP ne devront communiquer le NAVS qu'aux seuls exploitants d'un service utilisant un e-ID, eux-mêmes en droit d'utiliser le NAVS de manière systématique. Le fait que les IdP ne soient pas des autorités et qu'ils n'accomplissent pas non plus une tâche publique au sens strict ne doit pas les empêcher d'utiliser systématiquement le NAVS de la manière décrite. L'introduction d'un e-ID sous la forme exposée ci-dessus n'est donc pas remise en question par le présent projet de loi.

25 La stratégie peut être téléchargée à l'adresse suivante: www.egovernment.ch > Mise en œuvre > Stratégie suisse de cyberadministration.
26 Le Plan stratégique peut être téléchargé à l'adresse suivante: www.egovernment.ch > Mise en œuvre > Plan stratégique.
27 FF **2018** 4031 4105

1.4 Classement d'interventions parlementaires

La question de l'analyse des risques demandée par le postulat 17.3968 «Concept de sécurité pour les identifiants des personnes» est traitée au ch. 1.1.3 du présent message. Le classement du postulat est proposé.

2 Procédure préliminaire, consultation comprise

2.1 Avis de la Commission fédérale AVS/AI

La Commission AVS/AI approuve, sur le fond, une extension générale de l'utilisation systématique du NAVS aux autorités fédérales, cantonales et communales pour l'exécution de leurs tâches légales, tout en soulignant qu'elle attache une grande importance à la transparence de la nouvelle réglementation.

2.2 Procédure de consultation

Le 7 novembre 2018, le Conseil fédéral a chargé le DFI de mettre en consultation l'avant-projet de modification de la LAVS. Par courrier daté du même jour, le DFI a invité les cantons, les partis représentés à l'Assemblée fédérale, les organisations faîtières de l'économie et les associations et organisations intéressées à communiquer leur prise de position jusqu'au 22 février 2019. Le rapport relatif aux résultats de la procédure de consultation en fournit un résumé détaillé[28].

Sur le principe, la majorité des participants à la consultation ont approuvé l'inscription dans la loi d'une disposition autorisant de manière générale les autorités à utiliser le NAVS. Sur quelques points, leurs avis étaient toutefois partagés. Certains d'entre eux estimaient que les mesures techniques et organisationnelles ne devraient pas être réglementées au niveau de la loi. Quelques-uns tenaient aussi pour superflue la disposition prévue sur l'analyse des risques, d'autant que les concepts existants de protection des données prennent déjà en compte les risques éventuels résultant de l'appariement de données. Les participants ont rejeté quasi unanimement l'idée de rendre plus sévère la disposition pénale relative aux mesures techniques et organisationnelles, qui entraînerait des problèmes de délimitation insolubles. L'avant-projet a été modifié en conséquence. Pour le reste, le projet ne diffère de l'avant-projet que sur de rares points; les modifications en question sont d'ordre rédactionnel.

3 Comparaison avec le droit étranger

Si l'on observe l'ordre juridique d'autres États, on constate que les identificateurs de personnes peuvent être réglementés de façons très diverses. Alors que le système

28 www.admin.ch > Droit fédéral > Procédures de consultation > Procédures de consultation terminées > 2019 > DFI.

autrichien permet de dériver, du numéro de base d'un individu, des identificateurs de personnes spécifiques à des domaines, la Suède et d'autres pays scandinaves connaissent un identificateur de personnes unique, applicable à tous les domaines de la vie, qu'ils soient de nature publique ou privée. L'utilisation généralisée du numéro de sécurité sociale aux États-Unis s'explique quant à elle par le fait que ce numéro constitue le seul identifiant uniforme à l'échelle du pays (cf. 1.1.4).

4 Présentation du projet

4.1 Nouvelle réglementation proposée

Le projet propose que les autorités de la Confédération, des cantons et des communes puissent utiliser systématiquement le NAVS pour l'exécution de leurs tâches légales sans qu'une loi spéciale ne le prévoie. Cette possibilité découlera d'une disposition inscrite dans la LAVS qui servira d'autorisation générale, pour les autorités, à utiliser le NAVS de manière systématique. Il ne sera donc en principe plus nécessaire à l'avenir d'inscrire une norme potestative dans la loi spéciale correspondante pour chaque but d'utilisation et chaque catégorie d'utilisateurs. Le législateur aura néanmoins la possibilité de prévoir des identificateurs sectoriels de personnes pour certains domaines dans lesquels l'utilisation systématique du NAVS sera interdite.

La réglementation actuelle ne changera pas pour les services qui sont chargés d'accomplir des tâches administratives mais qui n'ont pas le caractère d'autorité. Ceux-ci auront toujours besoin d'une disposition spécifique dans une loi spéciale pour pouvoir utiliser systématiquement le NAVS. Les autorisations d'utiliser systématiquement le NAVS qui existent déjà dans la législation spéciale en vigueur seront maintenues. Une partie des dispositions en question font toutefois l'objet d'adaptations d'ordre rédactionnel. Comme dans le droit en vigueur, les établissements de formation pourront utiliser systématiquement le NAVS en vertu de la LAVS. Le projet précise cependant que le droit de le faire leur est reconnu. Ces établissements sont en effet chargés aussi bien de satisfaire à des obligations relevant du droit des assurances sociales que de remplir des tâches dans le domaine de la statistique fédérale. L'utilisation systématique du NAVS à des fins purement privées restera exclue. Par ailleurs, une importance suffisante sera accordée aux mesures de sécurité (pour plus de détails, cf. 4.2).

4.2 Mesures d'accompagnement

Le droit actuel contient déjà des prescriptions relatives aux mesures de sécurité qui touchent l'organisation, le personnel, l'infrastructure et la technique. Celles-ci se trouvent dans une ordonnance départementale[29]. Les principes essentiels seront à

[29] Ordonnance du DFI du 7 novembre 2007 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 (RS **831.101.4**).

l'avenir définis au niveau de la loi. Il s'agit de la réglementation des responsabilités, de la formation et de la documentation concernant la sécurité informatique, ainsi que de mesures visant à réduire au minimum les risques liés à l'accès aux données (cf. 1.1.3, analyse des risques). Il sera exigé de quiconque utilise systématiquement le NAVS qu'il établisse un concept SIPD. Autre prescription nouvelle, la Confédération et les cantons devront mener des analyses des risques afin de repérer et de prévenir tout risque de regroupement de bases de données non autorisé, notamment via des interfaces. Ils se fonderont pour ce faire sur des répertoires de bases de données qui utilisent le NAVS de manière systématique.

Le projet ne change rien aux dispositions existantes concernant l'échange de données. Il n'attribue pas non plus de nouveaux droits d'accès. Les droits actuels de consultation, de communication et de traitement de données ne sont donc pas étendus. Un échange de données entre autorités ne pourra se faire au moyen du NAVS que s'il existe une base légale explicite.

Le contenu des dispositions pénales existantes restera inchangé: quiconque utilise le NAVS de manière systématique sans en avoir le droit sera, comme aujourd'hui, puni d'une peine pécuniaire. Négliger de prendre des mesures techniques et organisationnelles continuera de constituer une contravention, qui sera punie d'une amende.

4.3 Pas d'obligation de revoir la conception de l'architecture des bases de données

Il ressort de l'expertise déjà mentionnée[30] que les données contenues dans différentes bases de données peuvent déjà être appariées avec une précision de 99,98 % à l'aide de quasi-identifiants (nom, prénom et date de naissance). Le gain de précision que pourrait apporter ici l'utilisation systématique du NAVS n'est donc pas déterminant au regard de la protection des données. Les problèmes fondamentaux sous cet aspect ne seraient donc pas non plus résolus par l'introduction de numéros sectoriels; ils ont généralement plutôt trait à l'architecture des bases de données, lorsque des données tant personnelles que factuelles sont enregistrées dans la même base de données. Sous l'angle de la sécurité de l'information, il faudrait, dans l'idéal, que le système informatique soit conçu de telle sorte que les données personnelles y soient exemptes de redondances et qu'elles soient enregistrées dans une autre base de données que les données factuelles relatives aux personnes concernées. Des attributs tels que le nom, le prénom, la date de naissance ou le NAVS devraient être enregistrés exclusivement dans une base de données unique. La mise en relation des données personnelles avec les données factuelles correspondantes ne devrait être possible qu'au moyen de «tables de liens» spéciales, tenues secrètes.

Une telle révision de la conception de l'architecture du système ne remettrait pas fondamentalement en question l'échange de données. Cependant, les attributs ne pourraient plus être enregistrés de manière décentralisée et l'accès aux données devrait donc toujours passer par la base de données centrale contenant ces attributs. Cela aurait pour effet d'intensifier le trafic réseau et d'augmenter le nombre d'accès

30 Cf. Basin, op. cit.

à ces bases de données, et ainsi d'accroître le risque d'erreurs. Les bases de données constitueraient des bouchons et des systèmes critiques qui devraient rester constamment disponibles. Concevoir et mettre en œuvre cette nouvelle architecture constituerait une tâche très lourde, impliquant des frais très élevés pour la Confédération, les cantons et les communes. En effet, comme on a pu le constater avec le bogue de l'an 2000, de petites modifications dans le format des données et la manière d'enregistrer et de traiter les données peuvent déjà avoir un impact considérable sur les coûts. Par ailleurs, l'élimination des redondances peut aussi entraîner des difficultés pour la gestion opérationnelle des bases de données concernées: sans redondances, il serait plus difficile de reconnaître et de corriger les erreurs éventuelles commises par les utilisateurs dans la saisie ou le traitement des données. En outre, en cas de perte de données, il n'est plus possible d'accéder à des copies redondantes; on est donc encore bien plus tributaire des sauvegardes que d'ordinaire. De plus, l'absence de redondances rendrait difficiles les tests de cohérence, aucune comparaison n'étant possible avec d'autres bases de données (redondantes).

Une disposition prescrivant la mise en place généralisée d'une architecture avec gestion séparée des données présenterait par conséquent de nombreux inconvénients et entraînerait des coûts élevés. Pour des groupes d'utilisateurs fermés – dans le domaine de la santé par exemple –, il peut tout à fait être judicieux d'installer au moment de la création d'une nouvelle base de données, dans des cas particuliers, une architecture impliquant une gestion minimale des données. Mais cela n'a de sens que si une telle nouvelle structure peut être mise en place d'un coup pour l'ensemble d'un grand groupe d'utilisateurs. Cependant, en général, les nouvelles bases de données créées sont isolées, ou les bases de données existantes sont complétées par de nouveaux attributs. Pour toutes ces raisons – difficultés opérationnelles et maigre plus-value d'un côté, coûts élevés de l'autre –, le projet ne prévoit pas d'obliger les utilisateurs du NAVS à remanier de fond en comble l'architecture de leur base de données. Ceux-ci resteront néanmoins libres de mettre en place une gestion séparée des données, s'ils le jugent utile et réalisable.

4.4 Aucune modification des dispositions relatives à l'obligation des autorités de garder le secret et à la communication de données

Le droit public suisse prévoit déjà que les autorités doivent, par principe, garder le secret sur les données personnelles dont elles disposent. Il ne peut être dérogé à ce secret de fonction que si une disposition légale autorise expressément les autorités à communiquer des données à d'autres autorités ou à comparer des données personnelles entre autorités. Le projet relatif à l'extension de l'utilisation systématique du NAVS ne change rien à ces principes. Il ne crée pas non plus de nouvelles bases légales concernant la collecte ou la communication de données. Là où la loi autorise la communication de données au moyen d'interfaces, le NAVS ne peut être communiqué comme information complémentaire que s'il existe une base légale formelle pour un tel échange de données. Il existe déjà dans le droit en vigueur certains domaines qui le prévoient, comme l'art. 32*a*^{bis} de la loi du 20 juin 1997 sur les armes. La nouvelle réglementation proposée pour l'utilisation systématique du

NAVS ne fera pas non plus augmenter le nombre d'appariements de données légalement admissibles. Comme c'est déjà le cas aujourd'hui, l'appariement ne sera admis qu'à condition qu'une loi le prévoie formellement, à l'instar de la loi sur la statistique fédérale ou de la loi du 22 juin 2007 sur le recensement[31].

4.5 Adéquation des moyens requis

Des émoluments pourront être perçus pour financer l'extension de l'utilisation du NAVS en dehors de l'AVS, de manière à couvrir les modestes coûts engendrés. Les ch. 6.1 et 6.2 présentent plus en détail les conséquences possibles du projet.

4.6 Mise en œuvre

Il faut que, comme actuellement, la CdC puisse percevoir des émoluments pour l'utilisation systématique du NAVS. Les modalités seront arrêtées au niveau du règlement. Il faut aussi que des exceptions à l'obligation de s'acquitter d'émoluments restent possibles. On peut aussi envisager des forfaits versés par les cantons en fonction de leur fréquence d'utilisation.

L'analyse des risques à effectuer régulièrement par les entités de la Confédération et des cantons en vertu de l'art. 153*e*, al. 1, P-LAVS pourra se faire dans le cadre des contrôles déjà prévus pour la protection des données: il faudra seulement y inclure un point supplémentaire portant sur l'utilisation systématique du NAVS. La gestion des répertoires au sens de l'art. 153*e*, al. 2, P-LAVS à prendre en compte pour l'analyse des risques est, au niveau de la Confédération, du ressort des départements. Les cantons et les communes détermineront eux-mêmes qui sera compétent pour la gestion des répertoires.

Les mesures d'accompagnement à respecter pour l'utilisation systématique du NAVS sont actuellement définies dans l'ordonnance du DFI. Les principes qui les régissent seront inscrits dans la loi.

5 Commentaire des dispositions

5.1 Loi fédérale sur l'assurance-vieillesse et survivants

Art. 49a, let. g

L'attribution d'un NAVS s'accompagne d'une inscription dans le registre central visé à l'art. 71, al. 4, let. a, LAVS. Mais on ne saurait en déduire systématiquement que la personne est assurée à l'AVS. C'est pourquoi le terme «numéro d'assuré» est supprimé au profit du seul «numéro AVS».

31 RS **431.112**

Par ailleurs, il faut savoir qu'il est prévu de supprimer le terme de «profil de la personnalité» dans le cadre de la révision totale[32] de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[33]. Au terme des débats parlementaires, il faudra veiller à coordonner les deux objets et modifier, le cas échéant, la phrase introductive en ce sens.

Art. 50d à 50g

Ces dispositions sont abrogées, la réglementation de l'utilisation systématique du NAVS en dehors de l'AVS étant déplacée dans une nouvelle partie de la LAVS, la quatrième.

Art. 87, par. 8, et 88, par. 4

Ces dispositions sont abrogées, car les dispositions pénales figureront dans la 4e partie de la LAVS.

Art. 89

La responsabilité solidaire de l'entreprise n'est pas conforme au principe du droit pénal selon lequel l'amende est strictement personnelle et intransmissible. Elle constitue dès lors une forme cachée de responsabilité pénale de l'entreprise. L'art. 79 de la loi fédérale du 6 octobre 2000 sur la partie générale du droit des assurances sociales (LPGA)[34], applicable à la 1re partie (art. 1, al. 1) de la LAVS, renvoie notamment à l'art. 6 de la loi fédérale du 22 mars 1974 sur le droit pénal administratif[35], applicable aux infractions commises dans une entreprise. L'art. 89 peut donc être abrogé à l'occasion de la présente modification.

Titre suivant l'art. 153a

Quatrième partie
Utilisation systématique du numéro AVS en dehors de l'AVS

Les règles en vigueur concernant la matière du présent projet se trouvent au chap. 4 (L'organisation) de la 1re partie (L'assurance). Du point de vue de la systématique législative, ce n'est pas adéquat, puisqu'il ne s'agit précisément pas de l'AVS et de son organisation, mais de l'utilisation du NAVS en dehors de l'AVS. Par souci de clarté et pour permettre de trouver plus facilement les dispositions applicables, il faut que l'utilisation systématique du NAVS en tant qu'identificateur de personnes en dehors de l'AVS soit réglée dans une partie distincte de la LAVS. C'est pourquoi une 4e partie, nouvelle (art. 153*b* ss), rassemblant les dispositions en question, est insérée directement avant les dispositions finales.

32 Message du 15.9.2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF **2017** 6565.
33 RS **235.1**
34 RS **830.1**
35 RS **313.0**

Art. 153b Définition

Cette disposition contient la définition légale de l'utilisation systématique, qui se trouve actuellement à l'art. 134bis du règlement du 31 octobre 1947 sur l'assurance-vieillesse et survivants (RAVS)[36]. Il convient, vu son importance, de l'inscrire dans la loi. Sur le fond, sa teneur reste inchangée. L'utilisation du numéro est réputée «systématique» lorsque des données personnelles sont liées à celui-ci et qu'elle concerne un groupe de personnes physiques clairement défini. Le critère décisif doit être que la partie essentielle et distinctive du NAVS soit entrée dans une base de données et y soit durablement enregistrée. Cela permet d'éviter que le contrôle de l'utilisation voulu par le législateur soit contourné par des modifications systématiques des numéros complets au moyen d'un système donné (par ex. omission du code du pays émetteur [756] formant les trois premiers chiffres du numéro, ajout d'une lettre ou d'un autre chiffre au numéro, cryptage).

Art. 153c Autorités, organisations et personnes habilitées

Al. 1: Cet alinéa énumère les instances admises à utiliser systématiquement le NAVS.

Let. a, ch. 1 et 2: Ces deux chiffres se réfèrent au niveau fédéral. La formulation s'inspire de la structure de l'art. 2, al. 1 à 3, de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[37], qui établit une distinction entre unités de l'administration centrale et unités administratives décentralisées.

Ch. 3: Aux niveaux cantonal et communal, il est également déterminant de savoir si une unité appartient ou non à l'administration. Les unités intercantonales ou intercommunales sont établies en dehors de l'administration. Si elles devaient être habilitées à utiliser systématiquement le NAVS, il faudrait, conformément au ch. 4, ajouter une base correspondante dans la convention intercantonale ou intercommunale instituant l'unité en question (cf. ch. 4).

Ch. 4: Ce chiffre vise les personnes et organisations de droit public ou privé qui accomplissent une tâche administrative, mais ne font partie ni de l'administration centrale ni de l'administration décentralisée. Si elles doivent pouvoir utiliser systématiquement le NAVS pour accomplir la tâche dont elles sont chargées, elles ont besoin d'y être autorisées par la loi spéciale correspondante. On peut citer, comme exemple concret, les prestataires reconnus de l'assurance obligatoire des soins et de l'assurance-accidents obligatoire, qui ne font partie de l'administration ni au niveau fédéral ni au niveau cantonal, mais qui sont chargés par la loi d'appliquer les assurances sociales en question. Il faut pour cela qu'à l'avenir, ils restent en droit d'utiliser systématiquement le NAVS; les bases légales le permettant existent déjà dans les lois spéciales respectives. Il en va de même pour l'application de la prévoyance professionnelle; les institutions de prévoyance pourront, comme actuellement, utiliser le NAVS de manière systématique. Les dispositions légales existantes à ce sujet restent inchangées.

36 RS **831.101**
37 RS **172.010**

Ch. 5: Actuellement, les établissements de formation cantonaux sont habilités à utiliser systématiquement le NAVS en vertu de l'art. 50*e*, al. 2, let. d, LAVS. Il faut qu'ils continuent de bénéficier de cette possibilité à l'avenir, d'une part, parce qu'ils jouent le rôle d'organes auxiliaires de l'AVS. Les étudiants des hautes écoles ainsi que les élèves du degré secondaire II (formation professionnelle duale ou à plein temps) et du degré tertiaire non universitaire (formation professionnelle supérieure) sont soumis à l'obligation de cotiser à l'AVS. Dans leur rôle d'organes auxiliaires, les établissements de formation concernés annoncent leurs étudiants aux caisses de compensation et procèdent, le cas échéant, à l'encaissement des cotisations (art. 29bis et 29ter RAVS). Pour que les cotisations versées soient comptabilisées correctement en faveur des personnes concernées, il faut joindre le NAVS au transfert de données. Par ailleurs, les écoles offrant un programme d'enseignement spécial (écoles spéciales) utilisent le NAVS dans le cadre de l'assurance-invalidité. Enfin, dans certains cantons, les écoles jouent pour les élèves le rôle d'organe d'exécution de l'assurance-accidents.

D'autre part, les établissements de formation doivent aussi remplir des tâches dans le domaine des statistiques de la formation, donc en dehors de l'AVS, lesquelles requièrent également l'utilisation du NAVS. Dans ces circonstances, il est judicieux d'accorder à l'avenir aussi aux établissements de formation, tant cantonaux que fédéraux, le droit d'utiliser systématiquement le NAVS pour l'exécution de leurs tâches dans ce domaine.

Let. b: Contrairement à l'application de l'assurance-maladie sociale et de l'assurance-accidents obligatoire, celle des assurances complémentaires régies par le droit privé ne constitue pas une tâche de l'administration. Il existe toutefois de nombreux liens entre les assurances complémentaires, d'une part, et les assurances maladie et accidents obligatoires, de l'autre. On ne peut donc pas considérer isolément leur application respective. C'est pourquoi l'art. 47*a* de la loi du 2 avril 1908 sur le contrat d'assurance[38] autorise déjà dans le droit en vigueur les prestataires d'assurances complémentaires à utiliser le NAVS de manière systématique. Cela doit rester possible à l'avenir. Cette règle, qui permet à des particuliers d'utiliser systématiquement le NAVS pour l'exécution d'une tâche régie par le droit privé, constitue une exception.

Pour le reste, l'utilisation du NAVS à des fins purement privées restera interdite, même si les personnes concernées donnent leur consentement à l'utilisation systématique de leur NAVS par des particuliers. Cette interdiction se justifie, du fait que la CdC ne peut pas imposer aux particuliers les contrôles de données et les corrections nécessaires en cas d'erreurs pour assurer la qualité des données comme elle le fait en vertu de l'art. 153*f*, let. b et c, pour les instances admises. Surtout, le risque d'appariements illicites de données serait sans doute nettement plus élevé si l'utilisation systématique était le fait de particuliers que lorsque le NAVS est utilisé par des autorités. Il en va de même en ce qui concerne le risque d'accès illicite aux fichiers de particuliers. Sous l'angle de la protection des données et de la sécurité de l'information, il s'impose donc de ne pas autoriser les particuliers à utiliser le NAVS.

38 RS **221.229.1**

Al. 2: Le législateur doit encore pouvoir, pour certains domaines, prévoir d'autres identificateurs de personnes que le NAVS. Il pourra donc à l'avenir aussi exclure l'utilisation systématique du NAVS pour des domaines donnés. On pense ici aux domaines dans lesquels des données sensibles au sens de l'art. 3, let. c, LPD sont concernées: il s'agit des données touchant les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'origine ethnique, les mesures d'aide sociale ainsi que les poursuites ou sanctions pénales et administratives.

Art. 153d Mesures techniques et organisationnelles

Les autorités, organisations et personnes habilitées à utiliser le NAVS de manière systématique doivent prendre les mesures techniques et organisationnelles nécessaires pour se prémunir contre toute éventuelle utilisation abusive. Ces mesures permettent de garantir la sécurité de l'information et la protection des données. Le présent article regroupe les obligations dont une partie figure actuellement dans 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 NAVS en dehors de l'AVS. Celles-ci sont actualisées et inscrites dans la loi.

L'obligation de diligence a pour but d'empêcher toute utilisation abusive du NAVS. Les autorités, organisations et personnes habilitées à utiliser le NAVS de manière systématique veilleront constamment à ce que les normes de sécurité applicables soient respectées. Les systèmes doivent en tout temps être conformes aux dernières prescriptions et être adaptés au besoin.

Let. a: Les droits d'accès aux bases de données qui contiennent le NAVS ne doivent être accordés qu'aux collaborateurs qui en ont besoin pour l'exécution de leurs tâches. Ces droits doivent être accordés de manière restrictive.

Let. b: Il importe de désigner une personne responsable de l'utilisation systématique du NAVS, qui devra prendre connaissance d'une manière vérifiable du concept SIPD visé à la let. d. Elle doit aussi avoir la compétence d'imposer les mesures qui sont nécessaires conformément au concept SIPD.

Let. c: Le NAVS ne doit pas être utilisé à d'autres fins que l'exécution des tâches prévues, ni être transmis à des tiers de manière non autorisée. Les cours de formation et de perfectionnement requis doivent informer les personnes ayant un droit d'accès qu'elles ne peuvent utiliser le NAVS que pour l'exécution des tâches qui leur sont confiées, et ne le divulguer à des tiers que si le droit le permet.

Let. d: Les autorités, organisations et personnes habilitées à utiliser le NAVS de manière systématique veilleront à ce que les opérateurs de leurs moyens informatiques et de leurs unités de mémoire établissent un concept de sûreté de l'information et de protection des données (SIPD) décrivant chacune des mesures de sécurité et de protection des données. Le concept SIPD devra désigner et analyser les facteurs de risque pertinents suivant les critères de disponibilité, de confidentialité, d'intégrité et de traçabilité. Il spécifiera par quelles mesures concrètes les exigences en matière de sûreté de l'information et de protection des données doivent

être mises en œuvre. Ces mesures se réfèreront à l'infrastructure, à l'organisation, à la formation du personnel ainsi qu'à l'adaptation du matériel et des logiciels.

D'une part, l'accès aux moyens informatiques et aux unités de mémoire doit être physiquement sécurisé. Si ces moyens et ces unités sont intégrés à des appareils portables, il importe de garantir, à l'aide de procédés cryptographiques correspondant à l'état de la technique, que les personnes non autorisées ne puissent y accéder.

D'autre part, cet accès doit être protégé par des mesures de sécurité informatique supplémentaires qui soient adaptées aux risques encourus et qui correspondent à l'état de la technique. Ces mesures comprennent au moins l'emploi de logiciels (antivirus), disponibles dans le commerce et à jour, de détection et d'élimination des maliciels, et le recours à des systèmes de pare-feu (centraux ou individuels). Il faut que les personnes qui peuvent accéder aux moyens informatiques et aux unités de mémoire soient tenues de s'authentifier au préalable. Si l'authentification requiert un mot de passe, celui-ci doit être tenu secret. Il ne doit pas être transmis et doit être modifié immédiatement si l'on soupçonne que des personnes non autorisées en ont connaissance. En outre, les logiciels d'exploitation et d'applications doivent faire l'objet de mises à jour de sécurité et d'élimination des erreurs (patches de débogage), autant que possible, dès que celles-ci sont disponibles. Les activités et événements importants sur les systèmes informatiques doivent être enregistrés et analysés régulièrement. Avant toute réparation, élimination ou destruction de moyens informatiques et d'unités de mémoire, il faut en outre s'assurer que ceux-ci ne contiennent plus ni NAVS ni autres données personnelles, et que ces données ne puissent pas être reconstituées.

Enfin, 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 et qui n'est pas soumis à un contrôle d'accès particulier (par ex. l'Intranet d'un service). Il est possible de parer audit risque en se conformant à l'état de la technique de cryptage.

Let. e: Il faut définir, dans un plan d'urgence, la manière de procéder en cas d'accès non autorisé aux bases de données ou d'utilisation abusive de celles-ci. La réglementation de ces mesures à prendre le cas échéant fait également partie du concept SIPD.

Art. 153e Analyse des risques

Al. 1: Les analyses des risques effectuées périodiquement visent à déceler les regroupements illicites de bases de données et, si nécessaire, à amener les administrations à collaborer de telle sorte que les mesures techniques et organisationnelles soient prises sur la base d'une évaluation réaliste et pertinente des risques systémiques globaux.

Les let. a et b définissent les entités qui, aux niveaux fédéral et cantonal, doivent procéder aux analyses des risques et pour quelles bases de données.

Al. 2: Les répertoires de bases de données qui contiennent le NAVS permettent de procéder de manière ciblée et coordonnée aux analyses des risques. Il est aussi

possible de faciliter la réalisation de cet objectif en faisant en sorte que les répertoires existants puissent faire l'objet d'une recherche avec pour critère «utilisation systématique du NAVS».

Art. 153f Obligations de collaborer

Les acteurs utilisant systématiquement le NAVS ont en outre à plusieurs égards l'obligation de collaborer avec la CdC. Ces obligations servent avant tout à garantir la fiabilité du NAVS.

Let. a: La CdC a besoin que les instances ayant le droit d'utiliser systématiquement le NAVS en dehors de l'AVS l'informent lorsqu'elles font usage de cette possibilité. Celles qui utilisent le NAVS en dehors de l'AVS seront également tenues de le signaler à la CdC, même en vertu du droit révisé. Cette obligation sera inscrite au niveau de la loi. À l'avenir, la CdC devra contrôler si l'unité qui annonce cette utilisation est une autorité ou une personne chargée d'exécuter une tâche administrative, visée à l'art. 153*c*, al. 1, let. a, ch. 4, auquel cas une base légale dans la loi spéciale est nécessaire.

Let. b et c: Ces obligations visent à garantir que la CdC puisse procéder à la vérification des NAVS utilisés et que les corrections qu'elle ordonne, le cas échéant, soient effectuées.

Art. 153g Communication du numéro AVS dans l'application du droit cantonal ou communal

Cette disposition correspond largement à l'art. 50*f* en vigueur. Par rapport au droit actuel, elle précise qui applique le droit communal et utilise systématiquement le NAVS, puisque ce dernier pourra aussi être utilisé pour l'application de ce droit. En vue de garantir la protection des données, la disposition définit à quelles conditions ces utilisateurs pourront communiquer le NAVS à des tiers dans des cas particuliers. À cet égard, il conviendra de toujours se référer aux conditions légales relatives à la communication de données qui s'appliquent au type d'activité concerné.

Dans leur teneur et leur présentation, les conditions relatives à la communication du NAVS par les organes fédéraux se fondent sur les dispositions similaires de la LPD.

Art. 153h Émoluments

Le droit en vigueur prévoit déjà que des émoluments peuvent être perçus sur la base de l'art. 46*a* LOGA pour le travail de la CdC qu'impliquent les tâches relevant de l'utilisation du NAVS en dehors de l'AVS. Comme l'utilisation systématique du NAVS en dehors de l'AVS est élargie, la possibilité de percevoir des émoluments est inscrite dans la LAVS afin d'accroître la transparence (cf. 6.1).

Art. 153i Dispositions pénales relatives à la quatrième partie

Al. 1: La nouvelle disposition correspond matériellement à celle de l'art. 87, par. 8, en vigueur. Comme actuellement, l'utilisation systématique non autorisée du NAVS sera punie par une peine pécuniaire.

Al. 2: Cette disposition reprend la règle de l'art. 88, par. 4, en vigueur. La contravention est réprimée, qu'elle ait été commise intentionnellement ou par négligence (art. 333, al. 7, du code pénal[39]).

Al. 3: Comme la LPGA n'est pas applicable à la 4e partie, un renvoi à l'art. 79 LPGA est nécessaire afin que les dispositions pénales susmentionnées soient applicables aux infractions commises dans une entreprise.

Titre précédant l'art. 154

Cinquième partie
Dispositions finales

Le projet règle l'utilisation systématique du NAVS en dehors de l'AVS dans une nouvelle 4e partie. De ce fait, les dispositions finales figureront dans une 5e partie.

Dispositions finales

Pour que les services et institutions qui utilisent déjà le NAVS de manière systématique puissent procéder aux changements nécessaires, il faut leur accorder un délai transitoire. Comme le droit en vigueur les oblige déjà à prendre des mesures techniques et organisationnelles, le délai d'une année est approprié.

Modification d'autres actes

Il importe de modifier ou d'abroger les normes relatives à l'utilisation systématique du NAVS en dehors de l'AVS inscrites dans d'autres lois, et d'éviter les redondances. Par ailleurs, diverses expressions utilisées sont par remplacées «numéro AVS».

5.2 Coordination avec d'autres projets de révision

Un besoin de coordination se fait sentir en raison du projet de révision en cours «Modernisation de la surveillance dans le 1er pilier et optimisation dans le 2e pilier de la prévoyance vieillesse, survivants et invalidité». Mais quel que soit celui des deux projets qui entrera en vigueur le premier («modernisation de la surveillance» ou présent projet), ce sont les modifications du projet «modernisation de la surveillance» qui seront déterminantes, sauf en ce qui concerne le remplacement du terme de «numéro d'assuré» par «numéro AVS» dans tout le texte de loi.

39 RS **311.0**

6 Conséquences

6.1 Conséquences financières et sur l'état du personnel pour la Confédération

La possibilité d'étendre l'utilisation systématique du NAVS fera augmenter, dans un premier temps, le nombre de demandes d'accès aux services proposés par la CdC. Il faut aussi s'attendre à ce que les utilisateurs envoient des demandes supplémentaires, ce qui provoquera une hausse des coûts de fonctionnement; il est toutefois difficile de prévoir dans quelle mesure. Ces coûts dépendront fortement du nombre de nouvelles entités qui souhaiteront utiliser systématiquement le NAVS et de leur comportement à cet égard. Au cours d'une période transitoire de deux à cinq ans, il faut s'attendre à une augmentation du nombre d'annonces faites par les utilisateurs et du nombre de demandes d'accès aux services proposés par la CdC. Ces charges supplémentaires pourront être assumées avec les ressources en personnel actuelles.

Un surcroît de dépenses sera également occasionné pour l'infrastructure de la base de données UPI, car le nombre d'utilisateurs influe sur la capacité des systèmes informatiques. S'agissant des coûts d'investissement pour moderniser les applications permettant de gérer les annonces d'utilisation systématique et celles donnant accès aux services mis à disposition par la CdC, ceux-ci devraient se situer entre un demi-million et un million de francs. L'estimation des coûts d'investissement pour une surveillance automatique accrue de l'utilisation des services mis à disposition se situe, elle, entre 200 000 et 750 000 francs. La fourchette des coûts totaux d'investissement va donc de 700 000 francs à 1,75 million de francs. Ces coûts seront financés par le budget ordinaire.

Comme dans le droit en vigueur, le Conseil fédéral pourra prévoir la perception d'émoluments pour les coûts supplémentaires liés à l'utilisation du NAVS en dehors de l'AVS. L'obligation de s'acquitter d'émoluments est réglée plus précisément aux art. 134^{sexies} et 134^{septies} RAVS. En pratique, comme de nombreuses exceptions sont prévues, presque aucun émolument n'est perçu. Les coûts qui ne sont pas financés par des émoluments sont supportés par la CdC ou par les fonds de compensation. Ces derniers sont financés principalement par les cotisations des assurés et des employeurs, par la contribution de la Confédération et par la TVA. Si la CdC fournit des services à des utilisateurs du NAVS étrangers à l'AVS, cela ne doit pas être aux dépens des assurances sociales du 1er pilier. Comme l'utilisation systématique du NAVS en dehors de l'AVS est élargie, la possibilité de percevoir des émoluments est inscrite dans la LAVS afin d'accroître la transparence. Un remaniement de la réglementation d'exception en vigueur devra se faire au niveau du règlement. Ainsi, les coûts de l'extension de cette utilisation pourront être répercutés sur ceux qui les occasionnent, à savoir les utilisateurs concernés.

Enfin, les gains d'efficience pour les autorités fédérales qui pourront désormais utiliser le NAVS contribueront à réduire les coûts. L'amélioration de la qualité des données facilitera et accélérera l'activité administrative des autorités. Elle permettra aussi d'échanger de manière simple, c'est-à-dire si possible automatique, des données entre autorités. Par ailleurs, habiliter de manière générale les autorités à utiliser le NAVS aura pour effet de rendre superflue la création d'une base légale spécifique pour chaque nouvelle utilisation. Les autorités législatives seront donc moins sollici-

tées. Par contre, les mesures d'accompagnement devront être mises à jour le cas échéant, ce qui pourra occasionner des frais supplémentaires. L'ampleur de ces économies et de ces dépenses supplémentaires ne peut pas être chiffrée.

6.2 Conséquences financières et sur l'état du personnel pour les cantons et les communes

Si des émoluments sont perçus pour l'utilisation systématique du NAVS, cela occasionnera des frais supplémentaires pour les cantons et les communes. Ceux-ci ne pourront être estimés qu'une fois connus le système d'émoluments et les clauses dérogatoires, mais ils devraient être minimes. En outre, l'obligation d'annonce entraînera pour les utilisateurs des frais initiaux, toutefois négligeables.

Cela dit, les gains d'efficience dans l'activité administrative (cf. 6.1) auront simultanément pour effet de réduire les coûts pour les cantons et les communes. Il est à présumer que les différentes autorités mettront en balance les coûts éventuels et l'utilité pour leur activité administrative, et qu'elles ne feront un usage systématique du NAVS que si le jeu en vaut la chandelle. On peut donc supposer que les conséquences seront positives pour les cantons et les communes. Les charges diminueront pour les autorités législatives des uns et des autres, puisqu'il ne sera plus nécessaire de créer une base légale spécifique pour chaque nouvelle utilisation. Par contre, comme pour les autorités de la Confédération, les mesures d'accompagnement devront être adaptées, ce qui occasionnera des frais supplémentaires qui ne peuvent pas être chiffrés.

6.3 Conséquences économiques

Aucune conséquence économique directe ne résultera du projet. En revanche, l'amélioration de la communication électronique entre citoyens et autorités, ainsi qu'entre les différentes autorités, aura indirectement des conséquences économiques positives, qu'il est toutefois impossible de quantifier.

6.4 Conséquences sociales

Le présent projet n'a aucune conséquence directe pour la société.

6.5 Conséquences environnementales

Le présent projet n'a aucune conséquence directe pour l'environnement.

7 Aspects juridiques

7.1 Constitutionnalité

7.1.1 Compétences

Le présent projet s'appuie sur les dispositions constitutionnelles qui régissent la compétence de la Confédération de légiférer dans le domaine de l'assurance-vieillesse et survivants (art. 111 et 112 Cst.). Dans la mesure où les réglementations sur le NAVS concernent l'utilisation de celui-ci comme identificateur de personnes pour des autorités, la compétence de la Confédération découle de l'art. 173, al. 2, Cst., qui confère à celle-ci la compétence de régler l'organisation des autorités fédérales. Si le législateur fédéral permet aux cantons et aux communes – sous réserve de dispositions différentes dans le droit cantonal – d'utiliser systématiquement le NAVS, il est également habilité à définir les conditions d'utilisation de cet instrument et à édicter les prescriptions correspondantes.

7.1.2 Protection de la personnalité

Le projet de loi est conforme à la Constitution également au regard de l'art. 13, al. 2, Cst. Les modifications de la LAVS proposées dans le présent projet précisent suffisamment les conditions dans lesquelles l'utilisation systématique du NAVS est admise. L'exigence d'une base juridique valide est donc satisfaite. Ces modifications respectent aussi le principe de finalité, puisque l'utilisation systématique du NAVS n'est admise que pour l'exécution des tâches légales. Le projet inscrit en outre dans la loi les mesures à prendre en matière de protection et définit les sanctions auxquelles s'exposent ceux qui ne les mettront pas correctement en œuvre (cf. 4.2).

7.2 Compatibilité avec les obligations internationales de la Suisse

Aucune des obligations de la Suisse en droit social international ne porte sur l'objet du présent projet.

7.3 Forme de l'acte à adopter

Aux termes de l'art. 164, al. 1, Cst., toutes les dispositions importantes qui fixent des règles de droit doivent être édictées sous la forme d'une loi fédérale. Le présent projet respecte cette règle.

7.4 Frein aux dépenses

Le présent projet n'est pas soumis au frein aux dépenses au sens de l'art. 159, al. 3, let. b, Cst., car il ne contient pas de dispositions relatives aux subventions et ne fonde ni crédit d'engagement ni plafond de dépenses.

7.5 Délégation de compétences législatives

L'art. 153*h* délègue au Conseil fédéral la compétence de prévoir des émoluments pour les prestations de services de la CdC liées à l'utilisation systématique du NAVS en dehors de l'AVS.