Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral des assurances sociales

Berne, le

Modification de la loi fédérale sur l'assurance-vieillesse et survivants (Utilisation systématique du numéro AVS par les autorités)

Rapport explicatif pour la procédure de consultation

Département fédéral de l'intérieur DFI
Inselgasse 1, 3003 Berne
Téléphone +41 58 462 80 41
Courriel info@gs-edi.admin.ch
www.admin.ch

Avant-projet
et rapport explicatif sur la modification de la loi sur l'assurance vieillesse et survivants (Utilisation systématique du numéro AVS par les autorités)

Condensé

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

Contexte

L'AVS utilise un numéro d'assuré depuis son instauration en 1948. À ce jour, cet identificateur personnel 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 révisées à cette occasion. Depuis lors, l'utilisation systématique du numéro AVS en dehors de l'AVS n'est autorisée qu'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 numéro AVS comme identificateur personnel permet d'actualiser des attributs personnels de manière automatique, précise et rapide en cas de changement d'état civil. La qualité des données contenues dans les registres d'utilisateurs est ainsi garantie. Grâce au fait qu'il est univoque, le numéro AVS 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'efficacité de l'administration en simplifiant les processus internes des autorités, de même que les procédures entre autorités. Avec le développement du traitement numérique des activités administratives, l'utilisation systématique du numéro AVS s'est beaucoup répandue depuis que la réglementation de 2008 est entrée en vigueur.

Si les dispositions actuelles de la loi fédérale sur l'AVS prévoient une telle utilisation par les autorités, elles la soumettent à des conditions qui ne sont pas toujours faciles à remplir. En outre, les pratiques législatives concernant l'autorisation d'une utilisation systématique du numéro AVS sont très disparates. Les cantons ne peuvent par ailleurs habiliter leurs autorités à utiliser le numéro AVS que pour l'exécution du droit cantonal. Pour toutes ces raisons, l'utilisation du numéro AVS comme identificateur personnel univoque est de plus en plus demandée par les autorités fédérales, cantonales et communales.

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 habilitation générale, sans avoir besoin à cette fin d'une disposition spécifique dans une loi spéciale pour chaque nouvel usage. La transparence sera accrue du fait que les conditions d'utilisation seront les mêmes pour toutes les autorités. De plus, la protection des données et la sécurité de l'information se verront accorder toute l'importance requise.

Il doit toutefois rester possible de prescrire dans les lois spéciales, à des fins particulières, des identificateurs sectoriels en lieu et place du numéro AVS. En ce sens, le législateur conserve sa liberté d'organisation. 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 numéro AVS pour autant qu'une disposition le prévoie dans la loi spéciale concernée. Par contre, l'utilisation systématique du numéro AVS à des fins purement privées restera exclue.

L'extension proposée de l'utilisation systématique du numéro AVS ne fait pas croître la vulnérabilité des systèmes d'information de la Confédération, des cantons, des communes ou d'autres utilisateurs admis, ni les risques d'abus. Le présent projet se limite à supprimer l'exigence actuelle d'une base légale spécifique pour chaque utilisation systématique du numéro AVS en habilitant de manière générale les autorités fédérales, cantonales et communales ainsi que certaines institutions d'utiliser systématiquement ce numéro.

Quiconque utilise le numéro AVS de manière systématique sera tenu, comme aujourd'hui, de garantir la protection des données. Afin de garantir également la sécurité de l'information, diverses mesures techniques et organisationnelles devront être prises. En premier lieu, il s'agira de protéger l'accès aux différentes banques de données afin de réduire le risque d'un usage abusif. Les prescriptions de sécurité relatives à l'accès aux banques de données qui contiennent le numéro AVS 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. Enfin, la loi sanctionnera non seulement quiconque utilise le numéro AVS sans prendre aucune mesure de précaution, mais aussi quiconque l'utilise sans faire preuve de la diligence requise ni se conformer aux règles de l'art.

Table des matières

Rapport explicatif

1 Présentation du projet

1.1 Contexte

1.1.1 Évolution de l'utilisation du numéro AVS

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 personnel 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 était insatisfaisante du point de vue de la protection des données. En outre, l'attribution des numéros AVS s'est heurtée au fil du temps à des goulets d'étranglement, ce qui a provoqué des problèmes considérables au niveau de la technique de l'information. La gestion des numéros AVS était devenue, qui plus est, source d'erreurs, car le numéro devait être modifié à chaque changement d'état civil. La création d'un identificateur fédéral de personne universel (IFPU) avait donc été proposée en 2003, à l'occasion de la procédure de consultation concernant la loi sur l'harmonisation des registres, adoptée par le Parlement le 23 juin 2006[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 personne (SPIN) gérés par un serveur central d'identification et de communication. Son intention était d'utiliser un identificateur uniforme pour chaque secteur administratif, dont la sécurité sociale. Toutefois, les résultats de cette consultation ont montré que le projet ne parviendrait pas à convaincre une 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 à l'échelle de la Confédération que des cantons, s'est beaucoup développée. Actuellement, la Centrale de compensations (CdC) compte près de 12 700 utilisateurs enregistrés. De plus, le NAVS est utilisé 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 mettre à disposition le NAVS en tant qu'identificateur de personne afin de faire avancer les projets de cyberadministration. L'utilisation d'un identificateur univoque rendrait l'administration plus efficace et améliorerait la qualité des banques 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.

Dans ce contexte, le Conseil fédéral a chargé en février 2017 le Département fédéral de l'intérieur de présenter une modification des dispositions de la LAVS afin de faciliter l'utilisation systématique du NAVS par les autorités fédérales, cantonales et communales dans l'accomplissement de leurs tâches légales.

En outre, lors des débats sur la modernisation du registre foncier[4], après qu'une analyse des risques[5] a été réalisée en septembre 2017, un postulat[6] chargeant le Conseil fédéral, notamment, de montrer de quelle manière il est possible de faire face aux risques liés à l'utilisation du NAVS en tant qu'identifiant unique des personnes a été déposé.

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 Normes constitutionnelles

La Constitution fédérale (Cst.)[7] garantit dans plusieurs dispositions différents éléments de la liberté personnelle. L'art. 13 Cst. protège tout particulièrement la sphère privée et ses diverses facettes contre les risques spécifiques qui la menacent. Ainsi, la protection des données garantie par la Constitution fait partie du droit au respect de la vie privée et de la sphère personnelle. Elle implique l'observation d'une série de principes régissant le traitement des données personnelles, en particulier les principes de finalité, de conformité au droit, de proportionnalité, d'exactitude et de bonne foi.

De plus, l'art. 13, al. 2, Cst. protège toute personne contre d'éventuels préjudices qu'elle pourrait subir en raison du traitement de ses données personnelles par l'État. Cette disposition s'applique aussi à l'utilisation d'identificateurs de personne. Dès son intégration dans la Constitution, elle a été controversée dans la doctrine. Le différend porte sur la question de savoir si l'on peut en déduire le droit subjectif de chaque individu à se déterminer sur les informations le concernant ou si la disposition doit être

[1] RS **431.02**
[2] RO **2007** 5259
[3] RS **653.1**
[4] 14.034 CC. Enregistrement de l'état civil et registre foncier
[5] David Basin, professeur de sécurité de l'information à l'EPF Zurich, « Risk Analysis on Different Usages of the Swiss AHV Number », 27 septembre 2017, cf. www.leprepose.ch > Protection des données > Statistique, registre et recherche > Numéro AVS (un résumé en français est disponible à la même adresse)
[6] Postulat 17.3968 de la Commission des affaires juridiques du Conseil national, « Concept de sécurité pour les identifiants des personnes »
[7] RS **101**

interprétée littéralement. La jurisprudence du Tribunal fédéral à ce sujet ne permet pas de trancher. Certains arrêts se fondent sur une interprétation littérale (par ex. arrêt IC_323/2015 du 8 janvier 2016), tandis que d'autres invoquent un droit individuel à se déterminer en matière d'informations personnelles (par ex. ATF *140* I 381). À ce jour, le Tribunal fédéral ne s'est pas prononcé sur cette question controversée. Dans la doctrine suisse récente, l'art. 13, al. 2, Cst. est interprété comme une instruction à l'adresse du législateur. Ce dernier doit prendre toutes les mesures nécessaires pour protéger les citoyennes et citoyens contre un emploi abusif des données qui les concernent. Il doit notamment veiller à ce que les autorités traitent les données personnelles avec toute la diligence qui s'impose.

1.1.3 Protection des données

La numérisation et l'utilisation systématique accrue du NAVS soulèvent des questions quant aux risques d'atteintes à la protection des données.

Le NAVS est une séquence de chiffres non « parlante », générée de manière aléatoire, à l'exception des trois premiers chiffres qui, conformément aux normes internationales, correspondent au pays émetteur. Pour le reste, le NAVS ne contient aucune information relative à son titulaire et ne permet de tirer aucune conclusion quant aux caractéristiques de sa personne. Sa seule fonction consiste à attribuer à l'individu concerné un jeu de données personnelles à l'intérieur d'une collection de données.

Cet attribut d'identification est employé en sus des attributs usuels (nom, prénom, date de naissance, etc.) exclusivement à des fins administratives. Il ne s'agit en aucun cas d'un code utilisateur donnant accès à toutes les informations personnelles. Ce n'est pas non plus un mot de passe permettant de s'introduire indûment dans des systèmes informatiques. Les mécanismes d'authentification des systèmes informatiques n'exploitent pas le NAVS comme un élément de la logique d'authentification. Son utilisation systématique ne rend pas les banques de données plus vulnérables. Les banques de données de la Confédération, des cantons et des communes sont organisées de manière décentralisée et ne peuvent pas être interconnectées entre elles grâce au NAVS. Les systèmes informatiques de ces administrations publiques emploient généralement des systèmes d'authentification à deux facteurs (*smartcard* de la Confédération, par exemple) pour l'accès aux applications bureautiques de base et imposent en plus des systèmes d'identification spécifiques (code utilisateur et mot de passe) pour ouvrir des applications spécialisées donnant accès notamment à des banques de données individuelles.

L'utilisation systématique du NAVS n'entraîne donc pas de risque supplémentaire de vol de données ou d'usurpation d'identité qui résulterait d'un usage abusif de l'identificateur. La possibilité d'un vol de données est davantage une question de sécurité informatique. La sécurité des systèmes informatiques, surtout lorsque ceux-ci contiennent des données personnelles sensibles, doit faire l'objet d'une attention minutieuse et permanente. La prévention des incidents nécessite une mise à jour constante des processus et des méthodes de sécurité. La présence éventuelle du NAVS parmi les données n'influe pas sur ces facteurs de risque. Le NAVS ne constitue pas non plus un document officiel d'identité et ne permet pas de produire une preuve recevable et formelle d'identité. Il ne dispense donc en rien les utilisateurs systématiques de cet identificateur d'un devoir légal de s'assurer au besoin de l'identité d'une personne en exigeant la présentation d'une pièce d'identité officielle. Au surplus, le NAVS ne donne en aucun cas accès sur simple présentation à une quelconque prestation des assurances sociales. Il n'y a donc pas d'intérêt, qu'il soit d'ordre pécuniaire ou immatériel, à voler le NAVS.

S'agissant des appariements, la combinaison éventuelle de données contenues dans plusieurs systèmes permettrait de regrouper plusieurs facettes d'une même personne (caractères de base, fisc, santé, justice, etc.) et donc de dessiner un profil de sa personnalité de manière plus ou moins détaillée en fonction des données disponibles. Cependant, pour effectuer ces appariements et combiner des données provenant de sources différentes, il serait nécessaire d'avoir accès à au moins deux banques de données établies par différentes autorités. Or il est rare que les systèmes officiels existants prévoient de tels accès multithématiques et, lorsque c'est le cas, une réglementation rigoureuse est mise en place. En effet, conformément au principe de proportionnalité, chaque service n'a accès qu'aux données dont il est responsable et pour lesquelles il est compétent selon une base légale claire. Le potentiel d'appariements entre différentes collections d'informations personnelles existe même en l'absence d'un identificateur tel que le NAVS. Tous les registres de personnes des autorités contiennent nécessairement des attributs d'identité tels que nom, prénom, date de naissance ou sexe. Ces attributs permettent déjà de relier facilement les données conservées dans différents registres. Grâce aux progrès rapides de l'informatique, les appariements de données sur la base de ces quelques caractères discriminants peuvent être réalisés aujourd'hui déjà avec une fiabilité de 99,98 %. Si des hackers parviennent à s'infiltrer dans deux banques de données des autorités, ou davantage, ils peuvent relier entre elles les données personnelles qui y sont contenues même sans disposer du NAVS. Le nombre d'appariements de données légalement admissibles n'augmentera pas avec la nouvelle réglementation proposée pour l'utilisation systématique de ce numéro. 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 sur le recensement. Par conséquent, l'utilisation systématique du NAVS ne compromet pas la protection des données et elle n'a pas non plus pour effet de rendre les citoyens « transparents ».

1.2 Dispositif proposé

1.2.1 Habilitation générale pour les autorités

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, de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants [LAVS][8]). L'utilisation systématique du NAVS repose 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 à l'utilisation du NAVS pour l'exécution du

[8] RS **831.10**

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 sont déjà habilités à utiliser systématiquement le NAVS en vertu de la législation sur l'AVS (art. 50*e*, al. 2, LAVS), sans qu'il soit 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 pour l'échange international de données 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.

Les services qui ne font pas partie des assurances sociales de la Confédération et qui souhaitent faire un usage systématique du NAVS doivent en informer préalablement la CdC. S'ils y sont habilités, la CdC leur ouvre l'accès à sa base de données UPI (*Unique Personal Identification database*), qui répertorie de manière univoque tous les titulaires d'un NAVS. Grâce à une comparaison régulière des données qu'elle gère avec celles des registres de personnes de la Confédération (notamment celui de l'état civil, Infostar, et celui des ressortissants étrangers et des requérants d'asile, SYMIC), la CdC peut garantir que celles-ci sont à jour, complètes et univoques. 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[9].

Le système actuel laisse au législateur le soin de décider de l'autorisation d'utiliser systématiquement le NAVS en dehors de l'AVS. Celui-ci prend sa décision sur la base d'une appréciation générale de la sécurité de l'information dans la matière réglementée par la loi spéciale en question.

Selon la solution proposée, les autorités de la Confédération, des cantons et – si cela est prévu par le droit cantonal – des communes doivent pouvoir utiliser systématiquement le NAVS pour l'exécution de leurs tâches légales sans qu'une loi spéciale le prévoie. Cette possibilité découlera d'une disposition inscrite dans la LAVS qui habilitera de manière générale les autorités à utiliser systématiquement le NAVS. Il ne sera donc plus nécessaire à l'avenir d'inscrire une norme dans la loi spéciale définissant chaque but d'utilisation et chaque utilisateur. Le législateur gardera néanmoins la possibilité de prévoir des identificateurs sectoriels de personne 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. Comme dans le droit en vigueur, les établissements de formation pourront utiliser systématiquement le NAVS en vertu de la LAVS. Le projet précisera cependant que le droit de le faire leur est reconnu. Ils sont en effet chargés d'accomplir des tâches relevant du droit des assurances sociales ou de celui régissant la statistique fédérale. Les dispositions légales en vigueur concernant l'autorisation d'utiliser systématiquement le NAVS seront adaptées. L'utilisation systématique à des fins purement privées restera exclue.

1.2.2 Mesures d'accompagnement

Aujourd'hui, les autorités travaillent avec nombre de bases de données qui composent leur capital informationnel. Le NAVS est une donnée supplémentaire qui complète aujourd'hui déjà ce capital ou qui viendrait le compléter selon la solution proposée. Ayant un intérêt évident à protéger leur patrimoine informationnel, les autorités sont tenues de prendre toutes les mesures en vue d'assurer la sécurité de l'information, sécurité informatique comprise. Cela vaut pour toute utilisation systématique du NAVS.

Pour éviter tout usage erroné et prévenir toute utilisation abusive, il faudra donc définir des lignes directrices efficaces, ainsi que des prescriptions d'ordre technique et organisationnel. On veillera tout particulièrement à ce que les bases de données soient protégées contre les consultations non autorisées et les manipulations. 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. Il est nécessaire de remédier à cette situation par des mesures de sécurité au niveau de l'organisation, du personnel employé, des infrastructures et de la technique, afin de parvenir à un niveau de sécurité suffisant. La mise en place de la sécurité informatique n'est pas une mesure isolée, mais un processus qui nécessite l'observation et l'adaptation constantes de divers facteurs.

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 doivent être consignées par écrit. Il importe de vérifier régulièrement les risques dans le domaine de la sécurité de l'information et il faut établir un concept de sûreté de l'information et de protection des données (SIPD). Au niveau de l'infrastructure, il s'agit en premier lieu de sécuriser physiquement l'accès aux moyens informatiques et aux unités de mémoire. Une autre mesure physique de sécurité consiste à garantir que les moyens informatiques et les unités de mémoire, avant toute réparation, élimination ou destruction, ne contiennent plus ni numéros AVS ni autres données personnelles, et que ceux-ci ne puissent pas être reconstitués.

Il importe par ailleurs de réduire au minimum, sur le plan technique, les risques d'accès non autorisé. Cela comprend la mise en place d'une procédure d'authentification appropriée et la prise de mesures de sécurité informatique (logiciel antivirus, système pare-feu). Les logiciels doivent correspondre aux dernières possibilités techniques 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 doivent être cryptées au moyen de procédés conformes aux dernières possibilités techniques. Enfin, l'analyse des identifiants de connexion des ordinateurs est élémentaire pour repérer les dysfonctionnements ou les incidents. Il est ainsi possible d'identifier les irrégularités dans le fonctionnement des systèmes informatiques qui sont dues à des programmes défectueux, à l'absence d'un programme ou à des failles de sécurité. Par ailleurs, il est nécessaire de concevoir et d'exercer à l'avance la gestion des incidents

[9] 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**

de sécurité. 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 dommages importants. Typiquement, les incidents de sécurité peuvent avoir pour conséquence l'espionnage, la manipulation ou la destruction de données. Pour prévenir ou limiter les dommages, ces incidents doivent être traités rapidement et efficacement. Les temps de réaction peuvent être réduits au minimum si une procédure à cet effet a été prescrite et testée avec succès.

Par ailleurs, la Confédération et les cantons doivent mener des analyses de risques dont le but vise à appréhender les risques de regroupement illicite de banques de données. Ils se basent pour ce faire sur des répertoires des banques de données qui contiennent le NAVS.

Quiconque utilise le NAVS de manière systématique sans en avoir le droit sera, comme aujourd'hui, puni d'une peine pécuniaire. Mais la disposition pénale relative à la prise de mesures techniques et organisationnelles sera plus sévère. Actuellement, est punissable uniquement celui qui ne prend pas de mesures du tout, alors que celui qui prend de telles mesures, mais de façon lacunaire, ne l'est pas. Cette lacune du droit en vigueur doit être comblée. À l'avenir, la disposition pénale inclura le fait de trop tarder à prendre les mesures techniques et organisationnelles, ou de le faire de manière incomplète, ce qui sera considéré comme une contravention et puni de l'amende. Les lignes directrices visant la protection des données et la sécurité de l'information s'en trouveront renforcées.

1.3 Appréciation de la solution retenue

1.3.1 Réponse au besoin d'adaptation des bases légales

La solution proposée apparaît équilibrée tant au regard de la pertinence que de la faisabilité et de la proportionnalité.

Le NAVS à treize chiffres est une séquence de chiffres unique, attribuée pour le restant de ses jours à toute personne physique peu après sa naissance sur territoire suisse ou lors de l'octroi d'un permis de séjour. Il permet une identification sans équivoque de la personne et contribue ainsi à améliorer la qualité des données, deux éléments qui préviennent des erreurs administratives coûteuses. Lors du traitement des données, l'utilisation systématique du NAVS facilite en particulier une mise à jour automatique, exacte et rapide des attributs de personne en cas de changement d'état civil. L'augmentation de la population et celle des tâches des administrations publiques se traduisent par un accroissement du volume des données et du nombre de mutations. À cela s'ajoute un nombre sans cesse croissant de noms complexes (par ex. doubles noms, noms écrits avec des caractères spéciaux ou dans une écriture non latine). Lorsque ces données sont traitées manuellement, ces facteurs peuvent être chronophages et la qualité des données peut être compromise. Le recours à un identificateur de personne sous forme de séquence de chiffres contribue notablement à résoudre ces problèmes.

L'utilisation systématique du NAVS permet aussi d'échanger des données entre autorités de manière simple et automatique. Les appariements de données prévus par le législateur et par conséquent licites, par exemple à des fins statistiques[10], produisent également des résultats plus précis quand ils peuvent être effectués au moyen d'un identificateur de personne univoque. Ces simplifications des processus internes et des processus entre autorités augmentent l'efficience administrative. Elles favorisent ainsi un usage efficace et économe des fonds publics, comme l'exigent l'art. 43*a*, al. 5, Cst. ainsi que l'art. 12, al. 4, 2e phrase, de la loi du 7 octobre 2005 sur les finances[11]. Les fonds publics sont également épargnés, puisque le travail législatif d'adaptation des lois spéciales n'est plus nécessaire.

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 sur l'annuaire officiel suisse. Si les personnes sont enregistrées dans une base de données avec un identificateur de personne univoque, tout 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. 1.1.2).

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 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 en cas de violation (cf. 1.2.2). L'obligation de prendre ces mesures devrait inciter les autorités qui utilisent le NAVS à maintenir leurs systèmes informatiques à jour. Le projet contribue ainsi à l'amélioration générale de la sécurité de l'information dans l'administration publique.

1.3.2 Autres solutions non retenues

1.3.2.1 Nouvelle conception de l'architecture des bases de données

L'Office fédéral de la justice et le PFPDT ont mandaté en mai 2017 un expert pour évaluer les risques résultant d'une utilisation systématique du NAVS. Dans son rapport[12], cet expert rappelle qu'aucun système ne peut être entièrement protégé contre les attaques. Si un hacker parvient à s'infiltrer dans plusieurs bases de données, il peut déjà apparier les données personnelles

[10] En vertu de l'art. 14*a* de la loi du 9 octobre 1992 sur la statistique fédérale (RS **431.01**).
[11] RS **611.0**
[12] David Basin, professeur de sécurité de l'information à l'EPF Zurich, « Risk Analysis on Different Usages of the Swiss AHV Number », 27 septembre 2017.

qu'elles contiennent avec une précision de 99,98 % à l'aide de quasi-identifiants (nom, prénom et date de naissance des personnes enregistrées). Si un identificateur de personne univoque tel que le NAVS est utilisé en plus, il n'en résulte pas, du point de vue du hacker, un gain de précision significatif. Au regard de la protection des données, l'utilisation systématique du NAVS par les autorités ne modifierait donc pas la situation de façon déterminante. L'expert expose en outre divers moyens 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. Toutefois, l'introduction d'identifiants sectoriels spécifiques ne serait pas utile à elle seule.

Si l'on entend écarter radicalement les problèmes liés à la protection des données, l'expert conseille 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'un assuré devraient 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, gardées secrètes.

Une telle révision de la conception des bases de données 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 toujours passer par la base de données centrale contenant ces attributs. Cela aurait pour effet d'intensifier le trafic de réseau et d'augmenter le nombre d'accès à ces bases de données, et ainsi d'accroître le risque d'erreurs. Les bases de données constitueraient des goulets d'étranglement et des systèmes critiques qui devraient rester constamment disponibles. Concevoir et mettre en œuvre cette nouvelle architecture constituerait une lourde tâche impliquant des frais très élevés pour la Confédération, les cantons et les communes. En effet, comme l'a montré l'expérience du bug 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. Si l'on élimine les redondances, il n'est pas possible d'accéder à des copies redondantes en cas de perte de données. On est alors encore bien plus tributaire des backups 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 prescription suivant laquelle la proposition de l'expert devrait être mise en œuvre partout entraînerait donc de nombreux désavantages et des frais élevés. Certes, pour des groupes d'utilisateurs fermés – dans le domaine de la santé par exemple –, il peut tout à fait être judicieux de prévoir, dans des cas particuliers, une architecture impliquant une gestion minimale des données au moment de la création d'une nouvelle base de 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. Dans tous les autres cas, on se contente de créer de nouvelles bases de données isolées, ou l'on complète les bases de données existantes par de nouveaux attributs. Pour toutes ces raisons – difficultés opérationnelles et faible plus-value d'un côté, coûts élevés de l'autre –, le présent projet évite d'exiger des acteurs utilisant systématiquement le NAVS qu'ils revoient de fond en comble l'architecture de leurs bases de données. Cependant, même si une prescription générale n'est pas inscrite dans la loi, ces acteurs resteront libres d'adapter cette architecture suivant la proposition de l'expert.

1.3.2.2 Procédure d'autorisation

L'option de mettre en place une procédure d'autorisation pour les acteurs utilisant systématiquement le NAVS a également été examinée. Dans un tel dispositif, le droit d'utiliser systématiquement le NAVS serait accordé par voie de décision par l'autorité compétente. Celle-ci devrait examiner dans chaque cas si le requérant est en mesure d'assurer la protection des données et la sécurité de l'information lors de cette utilisation. L'autorité requérante devrait notamment prouver qu'elle 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.

1.3.2.3 Numéros sectoriels

Dans un système fonctionnant avec des identificateurs sectoriels de personne coordonnés, 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 ex. 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 pas. Il faudrait donc commencer par les créer. À l'occasion de la consultation de 2004 sur le projet de loi SPIN, la plupart des cantons et des organisations a estimé qu'en ce qui concerne la cyberadministration, une sectorialisation serait trop complexe et coûteuse, qu'elle serait en plus source d'erreurs et qu'elle ne constituait par conséquent pas une solution praticable. Du point de vue actuel, une obligation générale d'introduire des identificateurs sectoriels de personne ou d'autres identifiants similaires représenterait pour de nombreuses autorités fédérales, cantonales et communales un retour en arrière, celles-ci ayant déjà pris des mesures et consenti des investissements dans la certitude que la réglementation actuelle (avec le NAVS comme identificateur de personne 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 personne particulier était souhaitée, cela resterait possible avec le projet proposé.

1.4 Analyse des avis donnés lors de la procédure de consultation

Le jj octobre 2018, le Conseil fédéral a chargé le DFI de mener une procédure de consultation relative à l'avant-projet de modification de la LAVS. Par courrier envoyé à la même date, 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 jj mmmm 2019. Les participants à la consultation ont réservé un accueil dans l'ensemble … à l'avant-projet. *Pour plus de détails, on se reportera à la synthèse des résultats de la procédure de consultation*[13].

1.5 Avis de la Commission fédérale AVS/AI

Un premier avant-projet a été soumis à la Commission AVS/AI le 29 juin 2017. Celle-ci 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.

1.6 Adéquation des moyens requis

Des émoluments peuvent être perçus afin de financer l'extension de l'utilisation du NAVS en dehors de l'AVS de manière à couvrir les modestes coûts engendrés. Le chap. 3 présente plus en détail les conséquences du projet.

1.7 Comparaison avec le droit étranger, notamment européen

Le droit social européen ne prévoit aucune disposition sur l'objet du présent projet.

2 Commentaire des dispositions

Art. 49a, let. g

L'attribution d'un NAVS a pour conséquence une inscription au registre central. On ne peut toutefois pas en déduire systématiquement que la personne est assurée dans l'AVS. C'est pourquoi le terme « numéro d'assuré » est supprimé au profit du seul « numéro AVS ».

Au surplus, il convient de signaler que dans le cadre du projet de révision totale[14] de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[15], il est prévu de supprimer la notion de « profils de la personnalité ». A la fin de la procédure parlementaire, il s'agira de veiller à assurer la coordination entre ces deux projets et, le cas échéant, de modifier la phrase introductive dans ce sens.

Art. 50a, al. 1, let. b^{bis}, 50c, 71, al. 4, let. a, et 93bis, al. 1

Ne concerne que le texte allemand.

Dans le texte allemand, le terme « *Versichertennummer* » est remplacé par « *AHV-Nummer* »,

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 4^{e} 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)[16], applicable à la 1re partie de la LAVS (art. 1, al. 1, LAVS), renvoie notamment à l'art. 6 de la loi fédérale du 22 mars 1974 sur le droit pénal administratif[17], applicable aux infractions commises dans une entreprise. L'art. 89 peut donc être abrogé à cette occasion.

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 avant-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

[13] www.admin.ch > Droit fédéral > Procédures de consultation > Procédures de consultation terminées > 2019 > DFI
[14] Message du 15 septembre 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.
[15] RS **235.1**
[16] RS **830.1**
[17] RS **313.0**

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 convient que l'utilisation systématique du NAVS en tant qu'identificateur de personne 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.

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)[18]. 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. 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 de la Confédération. 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[19], qui distingue entre unités de l'administration centrale et unités administratives décentralisées.

Ch. 3 : Au niveau des cantons et des communes, c'est le terme d'autorité au sens du droit cantonal qui est déterminant.

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. Ceux-ci ne font partie de l'administration ni au niveau de la Confédération ni à celui des cantons, mais ils sont chargés par la loi d'appliquer les assurances sociales en question. Il faut pour cela qu'ils restent, à l'avenir, 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.

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, qui 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[20] 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 constitue une exception, puisqu'elle permet à des particuliers d'utiliser systématiquement le NAVS pour l'exécution d'une tâche régie par le droit privé.

Pour le reste, l'utilisation du NAVS à des fins purement privées restera interdite, même si les personnes concernées donnent leur consentement. Cette interdiction se justifie du fait que la CdC ne peut pas imposer aux particuliers les contrôles de données et les corrections 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.

Al. 2 : Le législateur doit encore pouvoir prévoir, pour certains domaines, d'autres identificateurs de personne que le NAVS. Il pourra donc à l'avenir aussi exclure l'utilisation systématique du NAVS pour des domaines donnés. On pensera ici aux données personnelles sensibles au sens de l'art. 3, let. c, LPD. Il s'agit là 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 des mesures techniques et organisationnelles pour se prémunir contre d'éventuelles utilisations abusives. Cela permet de garantir la sécurité de l'information et la protection des données. Cet article regroupe les obligations dont une partie figure actuellement dans

[18] RS **831.101**
[19] RS **172.010**
[20] RS **221.229.1**

l'ordonnance du DFI sur les exigences minimales auxquelles doivent satisfaire les mesures techniques et organisationnelles à prendre par les services et institutions utilisant systématiquement le numéro d'assuré AVS en dehors de l'AVS[21]. 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 veillent 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 banques 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. Celle-ci doit signer le concept SIPD visé à la let. d ou en prendre connaissance d'une autre manière vérifiable.

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 veillent 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 doit 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 aux dernières possibilités techniques, 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 aux dernières possibilités techniques. Ces mesures comprennent au moins l'emploi de logiciels (antivirus), disponibles dans le commerce et régulièrement mis 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 tenus de s'authentifier au préalable. Si l'authentification requiert un mot de passe, celui-ci doit être gardé 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 numéros AVS 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 soumis à un contrôle d'accès particulier (par ex. l'Intranet d'un service). Il est possible de parer audit risque en recourant aux dernières possibilités techniques de cryptage.

Let. e : Il faut définir, dans un plan d'urgence, la manière de procéder en cas d'accès non autorisé aux banques 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 : Le but des analyses de risques effectuées périodiquement vise à appréhender les risques de regroupement illicite de banques de données et, si nécessaire, à coordonner la coopération entre les entités concernées afin que les mesures techniques et organisationnelles soient prises sur la base d'une évaluation réaliste et pertinente.

Let. a et b: Pour ce qui est de la responsabilité de mener les analyses de risques, les let. a et b énumèrent les entités qui y sont obligées et pour quelles banques de données.

Al. 2 : Les répertoires des banques de données qui contiennent le NAVS doivent permettre de procéder de manière ciblée et coordonnée. Ce but peut être soutenu en faisant en sorte que les répertoires de banques de données 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 une 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. C'est pourquoi le droit révisé maintiendra l'obligation d'annoncer ce type d'utilisation à la CdC. 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 au contraire un particulier chargé d'exécuter une tâche administrative, visé à l'art. 153*c*, al. 1, ch. 4, auquel cas une base légale dans la loi spéciale est nécessaire.

Let. b et c: La CdC doit être en mesure d'organiser des contrôles de données ou de faire procéder à de tels contrôles pour la vérification des numéros utilisés, ou d'ordonner des rectifications si nécessaire. Les instances qui utilisent systématiquement

[21] RS **831.101.4**

le NAVS devront prendre les mesures adéquates préconisées par la CdC pour s'assurer de la validité de celui-ci et des données personnelles qui y sont liées.

Art. 153g Communication du numéro AVS pour l'exécution du droit cantonal ou communal

Cette disposition correspond largement à l'art. 50*f* en vigueur. Le changement par rapport au droit actuel consiste dans le fait que l'utilisation systématique est étendue aux utilisateurs qui appliquent le droit communal, puisque le NAVS 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 en vigueur.

Art. 153h Emoluments

Selon le droit actuel, des émoluments peuvent déjà être perçus sur la base de l'art. 46*a* de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration[22] pour le travail de la CdC qu'impliquent les tâches relevant de l'utilisation du NAVS en dehors de l'AVS (cf. art. 134^{sexies} et 134^{septies} RAVS). Si la CdC fournit des services à des utilisateurs du NAVS étrangers à l'AVS, cela ne doit, à l'avenir non plus, pas être aux dépens des assurances sociales du 1er pilier. La possibilité pour le Conseil fédéral de prévoir des émoluments est donc maintenue. Comme l'utilisation systématique du NAVS en dehors de l'AVS est élargie, la possibilité de percevoir des émoluments est ancrée dans la LAVS.

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 et complète la règle de l'art. 88, par. 4, en vigueur. À la différence de la teneur actuelle, ce n'est pas seulement l'absence totale des mesures techniques et organisationnelles qui constituera une contravention, mais également l'absence partielle.

Al. 3 : Comme la LPGA n'est pas applicable à la 4^{e} 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 4^{e} partie. De ce fait, les dispositions finales figureront dans une 5^{e} 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 s'agira 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.

3 Conséquences

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

Une extension de l'utilisation systématique, par les autorités, du NAVS en dehors de l'AVS entraînera des charges supplémentaires pour la CdC. Elle fera en effet augmenter, dans un premier temps, le nombre de nouvelles annonces à traiter par la CdC, avec les accès aux services qu'elle propose. Un surcroît de dépenses sera également occasionné pour l'infrastructure d'UPI, car une augmentation du nombre d'utilisateurs influe sur la capacité des systèmes informatiques.

L'augmentation du nombre d'annonces sera de l'ordre de quelques dizaines au niveau de la Confédération, de plusieurs centaines au niveau des cantons et de plusieurs milliers au niveau des quelque 2220 communes. Potentiellement, plus de 10 000 annonces pourraient ainsi parvenir à la CdC. Cependant, les coûts supplémentaires ainsi générés devraient diminuer avec le temps. Leur niveau ne peut être déduit directement à partir de l'estimation du nombre d'utilisateurs supplémentaires, car il dépend aussi de la manière dont ces derniers s'acquitteront de leur obligation d'annonce (annonces individuelles ou collectives, répartition dans le temps). En outre, la gestion courante générera des coûts plus élevés en raison de l'augmentation du nombre de demandes. Le volume de ces coûts dépendra fortement du nombre de nouveaux utilisateurs du NAVS, ainsi que de la façon dont ces autorités recourront à l'utilisation systématique. Pendant une période transitoire de deux à cinq ans, il faudra compter avec une augmentation du nombre d'annonces d'utilisation et de demandes d'accès aux services offerts par la CdC. La charge supplémentaire sera absorbée par le personnel existant.

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, ils peuvent être estimés, à terme, à 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 par la CdC se situe, elle, entre 200 000 et 750 000 francs. La fourchette des coûts totaux d'investissement va donc de 700 000 à 1,75 million de francs.

Comme dans le droit en vigueur, le Conseil fédéral pourra prévoir la perception d'émoluments pour les coûts supplémentaires de la CdC liés à l'utilisation du NAVS en dehors de l'AVS. Ainsi, les coûts de l'extension de cette utilisation pourront être répercutés sur ceux qui les occasionnent, à savoir les utilisateurs concernés.

22 RS **172.010**

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 des autorités facilitera et accélérera l'activité administrative. Elle permettra aussi d'échanger simplement, c'est-à-dire si possible de manière automatique, des données entre les autorités. Par ailleurs, autoriser de manière générale les autorités à utiliser le NAVS aura pour conséquence qu'il ne sera plus nécessaire de créer une base légale spécifique pour chaque nouvelle utilisation. Les autorités législatives seront donc moins sollicitées. Par contre, les mesures d'accompagnement devront, le cas échéant, être mises à jour, ce qui occasionnera des frais supplémentaires. L'ampleur de ces économies et de ces dépenses supplémentaires ne peut pas être chiffrée.

3.2 Conséquences pour les cantons et les communes

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

Cela dit, les gains d'efficience dans l'activité administrative (cf. 3.1) 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.

3.3 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.

3.4 Conséquences sociales

Aucune conséquence sociale n'est à mentionner.

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

4.1 Relation avec le programme de la législature

Le 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.

4.2 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 leur 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-comporte 11 objectifs opérationnels. Son objectif opérationnel n° 7 est 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 reconnus 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 fédéral27 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 électroniques plus complexes puissent être mis au point, 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.

[23] FF **2016** 981
[24] FF **2016** 4999
[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** ...

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), si ceux-ci 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 à l'IdP d'utiliser systématiquement le NAVS, mais exclusivement dans ce but bien précis. En outre, les IdP ne devront communiquer le NAVS qu'aux seuls exploitants d'un service utilisant un e-ID, lui-même 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 qu'on vient d'exposer n'est donc pas remise en question par le présent projet de loi.

5 Aspects juridiques

5.1 Constitutionnalité et légalité

Le présent projet s'appuie sur les dispositions constitutionnelles qui régissent la compétence de la Confédération pour 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 son utilisation comme identificateur personnel pour des autorités, la compétence de la Confédération découle de l'art. 173, al. 2, Cst., qui confère à celle-ci la compétence de réglementer l'organisation des autorités fédérales. Si le législateur fédéral permet aux cantons et aux communes d'utiliser systématiquement le NAVS, il est également habilité à définir les conditions d'utilisation de cet instrument et à édicter les prescriptions correspondantes. Par contre, la Confédération n'a pas la compétence de réglementer les modalités des éventuels autres identificateurs de personne adoptés par les cantons. Ce sont ces derniers qui devront, à ce sujet, édicter les prescriptions légales relatives à la protection des données et à la sécurité de l'information.

5.2 Compatibilité avec les obligations internationales de la Suisse

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

5.3 Forme de l'acte à adopter

Conformément à 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.

5.4 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.

5.5 Délégation de compétences législatives

L'art. 153*g* délègue au Conseil fédéral la compétence de prévoir des émoluments pour les prestations de services de la Centrale de compensation liées à l'utilisation systématique de ce numéro en dehors de l'AVS.