Schweizerische Informatikkonferenz
Conférence suisse sur l'informatique
Conferenza svizzera sull'informatica
Conferenza svizra d'informatica

Expertise

Le numéro AVS comme identificateur de personnes uniforme et commun à toutes les organisations

Version 2.0, 03.10.2015

Cette expertise a été élaborée de

Berner
Fachhochschule BFH
E-Government-Institut

Auteurs: Brian Olivier, BFH
Brugger Jérôme, BFH
Dungga Angelina, BFH
Hefti Esther, Kt. ZH
Selzam Thomas, BFH
Spichiger Andreas, BFH
Weissenfeld Katinka, BFH

1 Management Summary

Cette expertise a été établie sur mandat de la Conférence suisse sur l'informatique (CSI). Les objectifs de l'expertise sont:

- d'illustrer, à l'aide d'exemples pratiques, les risques et les coûts qui résulteraient d'une non-utilisation du NAVS13 en tant qu'identificateur de personnes uniforme et commun à toutes les organisations
- de donner des informations sur les réglementations qui, à l'étranger, autorisent l'usage d'un identificateur de personnes standardisé à l'échelle nationale.

Des interviews ont été réalisées avec des responsables informatiques, des gestionnaires ou des chefs de service de l'administration publique suisse et avec des chefs de service des administrations publiques danoise, néerlandaise et espagnole. Au Danemark, le président d'un conseil indépendant d'experts s'est également mis à notre disposition pour une interview. Il s'engage en faveur de la protection et de la sécurité des données dans la communauté numérique danoise.
Dans sa première partie, cette expertise décrit l'usage qui est fait aujourd'hui du NAVS13 en Suisse, tout particulièrement les risques résultant d'une non-utilisation du NAVS13, ainsi que les réglementations en vigueur à l'étranger.
La seconde partie comprend une comparaison des systèmes, des considérations générales sur les risques, une analyse des implications sur la base de données et un examen approximatif des coûts.

Les résultats confirment la présomption que l'absence d'un identificateur univoque de personnes peut déboucher sur des situations à risque. Ils aboutissent sur le constat particulièrement surprenant que, lors des procédures administratives, le manque de clarté dans l'identification des personnes a notamment pour conséquence des atteintes à la protection des données. Les expériences menées à l'étranger montrent que l'utilisation d'un identificateur de personnes uniforme et commun à toutes les organisations est tout à fait compatible avec la protection des données et ne pose pas non plus de problème dans sa mise en application pratique.
Les réflexions menées sur des solutions alternatives montrent que la situation actuelle entraîne des surcoûts très importants. Les expériences menées à l'étranger confirment que l'identificateur de personnes standardisé est plus efficace. On a également fait la constatation que la Suisse dispose d'ores et déjà de l'infrastructure nécessaire pour la mise en service d'un tel identificateur.

Il est recommandé de résoudre de manière globale les problèmes d'identification qui surgissent dans de nombreuses procédures administratives, et non de manière individuelle et sectorielle. En l'absence de réelles alternatives, l'introduction du NAVS13 en tant qu'identificateur de personnes uniforme et commun à toutes les organisations est instamment recommandée.

2 Introduction

Il n'existe actuellement en Suisse aucun identificateur de personnes uniforme et commun à toutes les organisations. L'utilisation du numéro d'assuré AVS à 13 chiffres, le NAVS13, comme identificateur en dehors du champ des assurances sociales, requiert une base légale pour chaque utilisateur. Il en résulte des contraintes opérationnelles et des risques inhérents à l'absence de clarté lors du traitement des données dans les domaines extérieurs aux assurances sociales. Jusqu'à présent, l'introduction d'identificateurs de personnes standardisés et communs à toutes les organisations a toujours été entravée par des considérations qui relèvent de la protection des données.

La Haute École spécialisée bernoise (HESB) a reçu de la Conférence suisse sur l'informatique le mandat d'établir une expertise avec pour objectif, sur la base d'exemples simples et compréhensibles par tous, de mettre en lumière les dangers et les risques qui résulteraient de la non-utilisation d'un identificateur de personnes uniforme et commun à toutes les organisations. Elle expose également de manière succincte la situation et les réglementations en vigueur dans d'autres pays où un tel identificateur est utilisé.

Seront considérés ici des cas de figure relevés au sein de l'administration publique, dans lesquels un identificateur de personnes univoque est utilisé ou fait l'objet d'une demande. Mais ne sont décrits que des cas de figure dans lesquels un échange d'informations entre autorités est nécessaire en raison d'un mandat légal, et autorisé en raison de bases légales suffisantes.

Ce document présente d'abord la situation actuelle en Suisse concernant l'utilisation du numéro d'assuré AVSN13 en tant qu'identificateur uniforme de personnes. Au chapitre 4, on trouvera des cas de figure qui démontrent pourquoi, et dans quels cas, il est nécessaire, dans les procédures administratives, d'identifier les personnes avec un identifiant univoque. Concrètement, l'étude portera sur la situation dans l'assujettissement à la TVA des entreprises individuelles, dans le registre foncier, dans le casier judiciaire et dans le domaine des transports. Mais il ne s'agit que d'une modeste sélection d'innombrables procédures du même type. Les stratégies mises en place dans tel ou tel cas pour apporter des solutions, feront également l'objet d'un débat. Le chapitre 5 sera consacré aux réglementations qui ont été introduites dans des pays comparables au nôtre, en lien avec l'introduction à l'échelle nationale d'un identificateur de personnes uniforme et commun à toutes les organisations. Puis le chapitre 6 analysera les résultats, dans la perspective des risques, des coûts et de la protection des données. Il sera également procédé à une comparaison entre la situation de la Suisse et celle de l'étranger. Enfin, compte tenu des cas de figure relevés en Suisse et des expériences réalisées avec l'identificateur de personnes national au Danemark, aux Pays-Bas et en Espagne, l'expertise livrera ses conclusions et ses recommandations.

Conformément aux termes du mandat, les auteurs ont privilégié un langage facile à comprendre et accessible à tout le monde, l'objectif étant de présenter la situation de manière claire.

3. Situation actuelle

3.1 Introduction

Le NAVS13, le nouveau numéro d'assuré AVS à 13 chiffres, a été introduit en Suisse en 2008, pour remplacer l'ancien numéro à 11 chiffres. À l'origine, il a été conçu pour être utilisé dans le domaine des assurances sociales du premier pilier.

Par l'attribution d'un numéro univoque et non-parlant, il est le seul identifiant qui couvre l'ensemble de la population résidant en Suisse. Afin de garantir en continu l'attribution de numéros uniques et de contrôler l'univocité de tous les NAVS13, la Centrale de Compensation (CdC) a mis en place l'infrastructure et les procédures afférentes capables d'attribuer et d'utiliser

ces numéros. L'exploitation de cette infrastructure coûte chaque année aux contribuables et aux personnes soumises aux cotisations AVS/AI env. 5 millions de francs. À elle seule, son introduction a coûté env. 20 millions de francs en dehors des coûts de l'AVS/AI.

Ce chapitre présente la situation actuelle en relation avec l'utilisation du NAVS13 en tant qu'identificateur univoque de personnes en Suisse.

3.2 Le NAVS13

De nombreuses procédures administratives ont aujourd'hui un besoin impératif d'un identificateur univoque de personnes capable d'embrasser plusieurs organisations. Introduit le 1er juillet 2008, le numéro d'assuré AVS à 13 chiffres NAVS13 se prêterait bien à ce rôle, pour les raisons suivantes : [1]:

- Il est attribué à toutes les personnes résidant en Suisse[1];
- Dans la mesure du possible, l'univocité des numéros est garantie en permanence par le système de gestion qualité de la base de données ;
- L'attribution des numéros survient dans les plus brefs délais après la naissance ou après l'arrivée en Suisse;
- Le numéro ne se base pas sur des éléments d'identification personnels relevant de l'individu ; il ne permet donc pas de tirer des conclusions sur le titulaire du numéro (le numéro est dit *non-parlant*);
- En règle générale, il n'est attribué qu'une seule fois et reste valable également après le décès du titulaire.

3.3 La banque de données UPI

L'attribution et l'administration des numéros d'assuré NAVS13 incombe à la CdC [2]. Pour accomplir cette tâche, la CdC dispose d'un monopole et gère la base de données UPI. Pour procéder à l'attribution et à l'administration des numéros, l'UPI reçoit les informations dont elle a besoin principalement du Registre fédéral de l'Etat civil (unité Infostar) et du Système d'information central sur la migration (Symic) [3].

Les données contenues dans la banque de données UPI se résument aux termes génériques suivants :

- Nom de famille officiel;
- Nom de jeune fille;
- Prénom(s) officiel(s);
- Sexe;
- Date de naissance;
- Lieu de naissance;
- Nationalité;
- Noms de famille et prénoms des parents [4].

La désignation exacte des caractères et des types distinctifs figure dans le Catalogue officiel des caractères de l'Office fédéral de la statistique (OFS) [5]

3.4 L'utilisation du NAVS13

La base légale régissant l'utilisation du NAVS13 dans le domaine des assurances sociales figure dans les dispositions d'ensemble de la Loi fédérale sur l'Assurance vieillesse et survivants (LAVS).

[1] En cas de nécessité et sur demande, le système permet l'attribution d'un numéro également à des personnes qui ne résident pas en Suisse.

Elle précise que toute utilisation systématique du NAVS13 dans des domaines extérieurs aux assurances sociales requiert une base légale au niveau fédéral ou cantonal (LAVS Art. 50e) et doit être annoncée à la Centrale de Compensation (CdC).

Aujourd'hui déjà, une multitude d'autorités au niveau fédéral, ainsi que les caisses-maladie et les caisses de pensions (2e pilier) recourent aux prestations de la base de données UPI et utilisent le NAVS13 comme identificateur univoque de personnes dans leurs applications spécialisées. La liste des utilisatrices et utilisateurs systématiques du NAVS13 à la CdC compte actuellement env. 12'760 utilisateurs systématiques. [6]. On y trouve aussi bien les différents organes d'exécution de l'AVS que les institutions habilitées à utiliser le NAVS13 dans le cadre de la Loi sur l'AVS ou de la Loi sur l'harmonisation des registres. Hormis les institutions AVS, sont également habilités à utiliser le NAVS13 le Registre des habitants, l'Office fédéral de la statistique (OFS), les autorités fiscales, les organisations en lien avec la LPP et l'Armée. De plus, en vertu de l'Ordonnance sur la nouvelle carte d'assuré, les caisses-maladie [7] et les organismes en charge de l'aide sociale (Art. 50e de la LAVS) sont autorisés à utiliser le NAVS13. La majeure partie des institutions qui figurent dans la liste des utilisateurs est à classer dans le secteur de la formation.

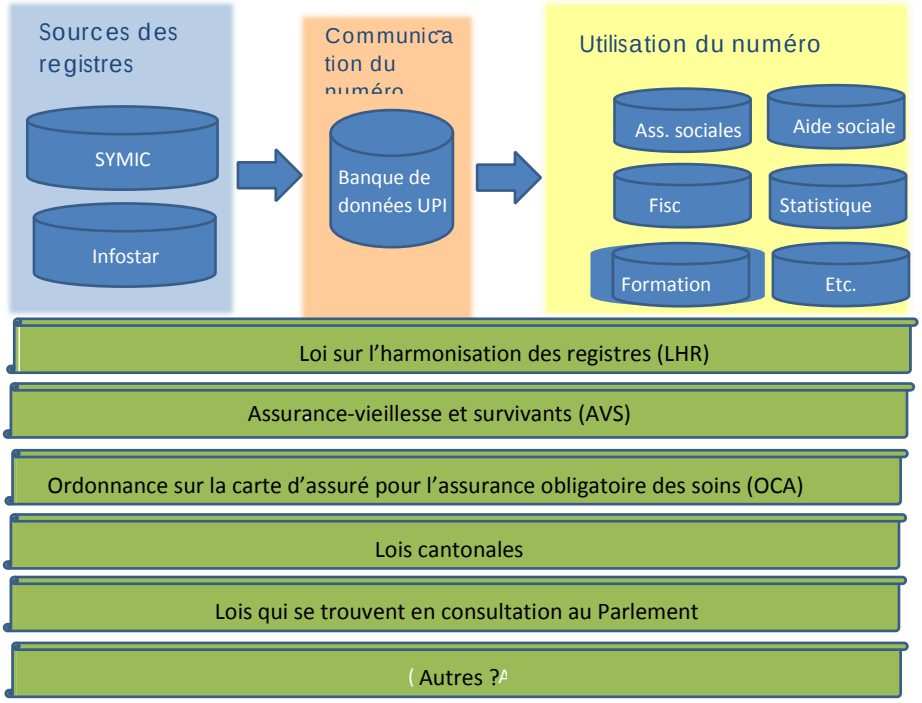


Illustration 1: Représentation modélisée du système actuel régissant le NAVS13 (Source: graphique élaboré par nos soins)

Le graphique 1 représente de manière simplifiée le système actuel en matière d'utilisation du NAVS13. La base de données UPI apparaît comme élément central: elle reçoit les données personnelles, procède à l'attribution des numéros et met ensuite les données à la disposition des utilisateurs légalement habilités. Ses principales sources sont les registres du SYMIC et d'Infostar[2].

Les éléments coloriés en vert affichent les bases légales intégrées dans le système.
Les dispositions qui concernent la tenue des registres figurent dans la LAVS et dans la Loi sur l'harmonisation des registres (LHR). Les dispositions concernant l'utilisation des numéros figurent dans une multitude de lois. Toutes les instances habilitées à les utiliser et toutes les lois

[2] Pour réduire la complexité de l'information, le graphique renonce à nommer tous les registres concernés et ne représente que les deux registres qui sont les principales sources.

afférentes ne figurent pas sur le graphique. L'habilitation à utiliser les numéros à 13 chiffres figure en partie dans d'autres textes de loi.

3.5 La protection des données

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) suit attentivement les discussions sur l'utilisation du NAVS13, et cela déjà depuis son introduction. Il estime que l'utilisation du numéro d'assuré AVS à 13 chiffres dans des domaines extérieurs aux assurances sociales n'est pas sans risques pour la protection des données. Le PFPDT redoute surtout que certains n'utilisent ces données personnelles pour procéder à des appariements abusifs et contraires à l'objectif visé.

Les dangers liés à l'utilisation d'un identificateur de personnes uniforme et commun à toutes les organisations ont été exposés en 2002 dans un avis de droit du professeur et docteur en droit Giovanni Biaggini [8]. Son expertise parvient à la conclusion que l'introduction d'un identificateur de personnes uniforme et commun à toutes les organisations représente un danger particulièrement élevé pour la confidentialité de données liées au vote électronique, de données médicales et de données en rapport avec des poursuites et des sanctions pénales. Il redoute également que des données personnelles soient collectées dans des bases de données sans que les personnes concernées n'en aient connaissance, celles-ci perdant ainsi toute souveraineté sur des données qui leur appartiennent en propre.

L'expertise fait remarquer que l'introduction et l'utilisation d'un identificateur de personnes uniforme et commun à toutes les organisations ne se justifie que pour répondre à un intérêt public supérieur. Il doit également respecter le principe de proportionnalité et satisfaire aux impératifs pertinents du droit constitutionnel. L'intérêt public supérieur légitime-t-il en l'occurrence un assouplissement de l'affectation originelle, et cet assouplissement répond-il au principe de proportionnalité ? L'expertise ne tranche pas. Si le critère de l'intérêt public réclame d'être à chaque fois pesé en fonction du contexte, celui de la proportionnalité requiert, quant à lui, la démonstration de sa nécessité. Concrètement, il s'agit d'estimer s'il existe des alternatives viables. [8]

Selon le PFPDT, la mise en place d'un identificateur de personnes pour l'ensemble des organisations faciliterait techniquement l'usage abusif de données liées à la personne. La non-utilisation d'un identificateur de personnes uniforme et commun à toutes les organisations serait seule de nature à écarter tout risque d'appariement illicite de données. [9]. Cette position n'a pas varié depuis l'introduction du NAVS13, comme le confirme un communiqué de presse du PFPDT rendu public le 16.04.2014 [10].

3.6 Efforts visant à systématiser l'utilisation du NAVS13

À l'heure actuelle, trois messages parlementaires réclament l'usage systématique du NAVS13 [3].

Dès qu'une autorité est appelée à échanger des données à caractère personnel avec une autre autorité ou, en interne, à se connecter avec un autre système informatique, elle doit se demander :

1. si elle a pour objectif de créer une base légale pour l'utilisation du NAVS13;
2. si elle planifie la création d'un identificateur de personnes propre à son domaine ;
3. ou si elle veut effectuer le travail d'identification manuellement

[3] Message du 20 juin 2014 relatif à la loi sur le casier judiciaire (SR 14.053) ; Message concernant la modification du code des obligations (Droit sur le registre du commerce) du 15 avril 2015 (SR 15.034) ; Message du 16 avril 2014 concernant la révision du code civil suisse (Enregistrement de l'état civil et registre foncier) (SR 14.034) [6] La liste des personnes qui ont pris part aux interviews se trouve dans les annexes.

Les cas de figure traités dans le chapitre ci-après démontrent que la non-utilisation d'un identificateur de personnes uniforme et commun à toutes les organisations comporte des risques et entraîne des coûts.

4 Cas de figure

Les informations recueillies pour les cas de figure ci-après proviennent d'interviews d'une heure accordées par les responsables informatiques, les chefs de service et les administrateurs des autorités correspondantes. Mais il ne s'agit ici que de quelques cas, choisis pour illustrer les contraintes et les risques. Multiplier les exemples analogues eût dépassé le cadre de cette expertise. Les présents cas de figure mettent tous en lumière les difficultés, liées à l'identification de personnes, que rencontrent les autorités dans l'accomplissement de leur fonction légale.

4.1 Assujettissement à la TVA au sein des entreprises individuelles

4.1.1 Situation initiale et description du cas de figure

La bonne perception et l'encaissement de la taxe sur la valeur ajoutée relève de la Division principale de la TVA au sein de l'Administration fédérale des contributions (AFC) [11].

Dans les entreprises individuelles, ce sont les personnes, et non les entreprises, qui sont enregistrées. Dans la restauration, par exemple, il arrive souvent que la personne enregistrée fasse faillite. Nous noterons au passage que ce n'est pas l'entreprise individuelle qui est concernée, mais bien la personne enregistrée. Si, par la suite, cette personne entend ouvrir un nouvel établissement, il est très difficile de découvrir si, dans un contexte ou un autre, elle a encore des impayés.

Illustration. Monsieur Meier gère le restaurant du Rössli. L'autorité chargée de la collecte de la taxe sur la valeur ajoutée remarque que Monsieur Meier na pas déduit de TVA pour son établissement. Mais entre-temps, M. Meier a dû fermer son restaurant. Il ne peut pas honorer sa facture ouverte de TVA. Une procédure de faillite est engagée contre lui. Quelque temps plus tard, le même Monsieur Meier se remet dans la restauration et reprend le Löwen. Il annonce son établissement à l'autorité de perception de la TVA, qui accepte l'inscription sans savoir que Monsieur Meier a encore des factures impayées auprès d'elle.

À l'heure actuelle, pour empêcher de tels cas il en coûte beaucoup de temps et d'argent à l'autorité de perception de la taxe sur la valeur ajoutée. Des affaires comme celle-là génèrent pour elle un préjudice financier tout à fait concret.

L'autorité de perception de la TVA éprouve également les pires difficultés dans les cas où une personne possède plusieurs entreprises, qui peuvent présenter des formes juridiques différentes. Lorsqu'elle traite un dossier, l'autorité n'est pas en mesure de voir si cette personne a encore des dettes non réglées dans une autre affaire.

Remboursements
Pour les ressortissants étrangers, le remboursement de l'impôt anticipé s'effectue au niveau fédéral : ils sollicitent le remboursement de cet impôt par le biais d'un formulaire. Là également, il s'agit pour l'administration fiscale d'un processus coûteux en temps et en argent pour détecter si cette personne a encore des impayés au Service des contributions. C'est la raison pour laquelle, dans les affaires de remboursement à des ressortissants étrangers, l'identification joue un rôle important.

Les mêmes contraintes surviennent dans le domaine de la fraude fiscale et dans le cadre de l'échange automatique d'informations.

L'échange d'informations avec d'autres autorités administratives dans un contexte d'identificateurs univoques de personnes, est plutôt restreint. À l'heure actuelle, l'Administration fédérale des contributions (AFC) reçoit les données émanant des registres des faillites, ainsi que le numéro d'identification (IDE) des entreprises individuelles qui figurent dans le registre IDE. De son côté, l'AFC ne transmet des données fiscales aux autorités d'enquête compétentes qu'en cas d'infraction pénale. Le besoin d'un identificateur univoque de personnes se fait donc surtout sentir à l'intérieur même de l'AFC, lors de procédures administratives.

4.1.2 Conséquences d'une non-utilisation du NAVS13

Dans le seul cadre de l'assujettissement à la TVA des entreprises individuelles, le préjudice financier peut se chiffrer en millions de francs.

Actuellement, la probabilité de parvenir à l'identification univoque de personnes est très faible. Aujourd'hui, l'identification par le biais du patronyme et de la date de naissance n'est en effet plus univoque. Une partie du problème réside dans le fait qu'en Suisse les noms sont modifiables. Par conséquent, à part le NAVS13, il n'y a plus aucune constellation en Suisse susceptible de permettre l'identification univoque d'une personne.

Dans beaucoup de procédures, l'AFC a aujourd'hui mis en place un contrôle professionnel des demandes. Concrètement, les formulaires qui lui sont soumis sont adressés à un employé. Celui-ci vérifie si de l'argent a déjà été versé à la personne assujettie, ou si plusieurs requêtes sont en suspens pour cette personne. Ces vérifications s'effectuent manuellement et compliquent de manière importante le processus de traitement. L'employé(e) doit en effet partir manuellement à la recherche de redondances dans une base de données qui contient 600'000 personnes/entreprises.

Pour accomplir pleinement son mandat légal, l'Administration fédérale des Contributions doit donc faire face à un véritable défi. Cette situation a déjà fait l'objet de discussions dans le cadre des révisions régulières effectuées par le Contrôle fédéral des finances (CDF) [12]. Dans ses rapports, celui-ci fait par exemple observer que, dans les paiements, le risque existe que le montant soit versé deux fois à la même personne. À l'heure actuelle, ce cas de figure ne peut être contrôlé qu'au moyen du compte de paiement. Pour répondre aux exigences du CDF, l'AFC met en place des mesures organisationnelles, au lieu d'instituer des mesures techniques.

4.1.3 Travaux en cours et perspectives

Les problèmes mentionnés plus haut apparaissent dans presque tous les processus de recouvrement et de remboursement. C'est pourquoi il est prévu d'instituer des systèmes qui permettront d'accroître leur efficacité d'env. 30-40%. Il s'agit d'un logiciel de *matching* des données. S'il y avait un identificateur univoque de personnes, on pourrait faire l'économie de toutes ces mesures.

La saisie des données personnelles s'effectue aujourd'hui sur la foi d'une auto-déclaration de la personne concernée. Pour les nouveaux assujettissements à la taxe sur la valeur ajoutée, l'AFC interrogera désormais le NAVS13.

À partir de là, la discussion est ouverte sur la légalité de cette démarche. L'insécurité qui se présente ne réside pas dans le fait d'interroger le numéro à 13 chiffres, mais dans son utilisation. Dans les appariements de données, la légalité n'est pas toujours évidente. Dans la législation actuelle, il n'apparaît pas toujours clairement si, par exemple, il est permis de prendre en considération des informations qui ressortissent du domaine de la TVA pour traiter un cas de remboursement. Même si les bases légales existent, il existe un flou dans l'interprétation concrète des lois existantes.

Du point de vue de l'administration fiscale, l'institution d'un identificateur de personnes est clairement un besoin. Peu importe comment cet identificateur est conçu. Pour le domaine des contributions, on pourrait imaginer l'introduction d'un numéro d'identification fiscale pour toutes les personnes soumises à l'impôt fédéral.

Autre aspect du problème : dans l'optique de l'échange automatique d'informations entre états, l'utilisation du NAVS à 13 chiffres comme identificateur univoque de personnes est une exigence trop fortement liée aux frontières nationales. L'aspect international est ainsi entièrement occulté. Quel numéro un pays utilise comme identificateur est une question qui devrait se régler au niveau international, et les critères de ce numéro doivent faire l'objet d'un accord international. On pourrait par exemple imaginer que le NAVS13 qui vaut pour la Suisse, soit utilisé comme identificateur de personnes reconnu sur le plan international.

4.2 Cas de figure: le registre foncier

4.2.1 Situation initiale et description d'un cas de figure

Les registres fonciers suisses sont ainsi conçus qu'ils se basent sur le bien immobilier: il n'existe aucun registre foncier central pour toute la Suisse. En cas de besoin (par ex. héritage, blocage des avoirs de potentats), la propriété des biens-fonds est établie au moyen d'un registre accessoire (*resp*. au moyen d'une liste des divers offices du registre foncier) qui est tenu d'après les communes ou d'après les arrondissements des registres fonciers. [13]. Pour la saisie uniforme entre autres de données personnelles dans tous les registres fonciers, l'Office fédéral de la justice (OFJ) a adopté en 2011 un modèle de données [14] qui est aujourd'hui implémenté. Il définit les caractéristiques personnelles suivantes: nom, prénom, date de naissance, sexe, lieu d'origine ou nationalité. La saisie de ces données personnelles s'effectue toujours au moment de l'achat du bien-fonds. Mais souvent ces données ne sont pas actualisées, car dans le domaine des registres fonciers, c'est le principe de la demande qui prévaut : les données ne peuvent être modifiées que sur la demande expresse de la personne concernée. Depuis le 1.1.2012, les données personnelles peuvent être vérifiées au moyen d'une copie du passeport ou de la carte d'identité. (Art. 51 ORF).

Aujourd'hui, il est impossible de voir qui possède quels biens-fonds en Suisse. Si, par exemple dans le cadre d'un délit, l'enquête nécessite de connaître le nombre total des biens-fonds d'un propriétaire, cela occasionne aujourd'hui de gros frais, et ce n'est même pas toujours possible. La gestion décentralisée du registre foncier et l'absence d'infrastructures techniques rendent extrêmement difficiles les recherches sur la propriété au niveau national. Les recherches doivent s'effectuer de manière séparée, dans chaque registre foncier. De plus, elles s'appuient sur les caractéristiques personnelles mentionnées plus haut. Mais comme il n'y a aucune contrainte d'actualiser les données personnelles qui figurent dans les registres fonciers, les données personnelles d'une seule et même personne peuvent s'y trouver saisies différemment d'un registre à l'autre, et cela malgré le modèle de données uniforme. Cette disparité dans l'actualité des données s'explique également par l'évolution historique de la collecte des caractéristiques personnelles. La saisie complète de ces caractéristiques, telles qu'elles figurent dans le modèle de données évoqué plus haut, n'est exigée que depuis 3 ou 4 ans. Auparavant, la seule indication du nom suffisait, mais graduellement d'autres caractéristiques ont été exigées, comme la date de naissance ou le lieu d'origine.

La disparité dans l'actualité des données a pour conséquence que, dans certains cas, la même personne est enregistrée différemment au gré des divers registres, ce qui rend impossible toute détection (détection impossible par manque de compatibilité).

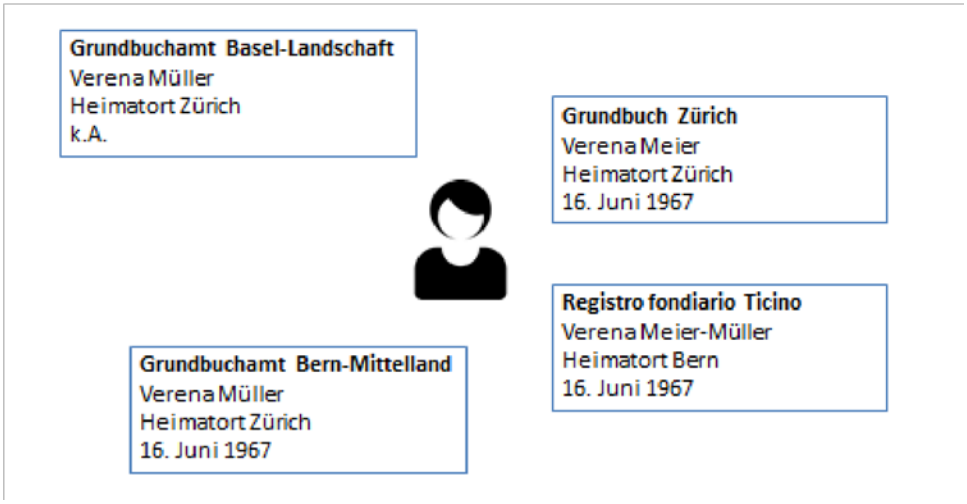


Illustration 2 : détection impossible par manque de compatibilité

Le tableau 2 illustre un cas fictif d'impossibilité d'une détection par manque de compatibilité. Madame Verena Müller, née le 16 juin 1967, achète un bien-fonds dans le canton de Bâle-Campagne. Elle n'indique pas sa date de naissance, car à cette époque ce n'était pas exigé. Quelques années plus tard Madame Müller souhaite déménager à Berne et se décide pour l'achat d'un appartement en propriété au centre-ville. À cette occasion, elle donne sa date de naissance. À Berne, Madame Müller rencontre son futur mari, Monsieur Meier, dont elle prend le nom de mariage. Désormais, dans toutes les démarches administratives, elle utilise le nom de Verena Meier. Conséquence du mariage: son deuxième lieu d'origine est désormais Berne. Par la suite, elle acquiert encore deux biens-fonds, l'un dans le canton de Zürich, l'autre au Tessin. Tandis que, par pure habitude, elle fait inscrire dans le registre foncier zurichois « Zürich » comme lieu d'origine, lors de son acquisition au Tessin elle fait inscrire son deuxième lieu d'origine, Berne. Seule l'utilisation d'un identificateur univoque de personnes est en mesure d'assurer de manière claire la compatibilité de ces quatre inscriptions.

Illustration 3: Fausse compatibilité

De fausses compatibilités peuvent également conduire à des confusions. Le tableau 3 montre un exemple possible de fausse compatibilité. Ici, la seule possibilité de déceler qu'il ne s'agit pas de la même personne est de consulter les numéros AVS.

4.2.2 Conséquences d'une non-utilisation du NAVS13

Les cas de Madame et de Monsieur Müller illustrent combien il est difficile d'identifier des propriétaires qui figurent dans différents registres fonciers. Sans un identificateur univoque de personnes, la fausse compatibilité dans le cas de Monsieur Müller, comme la compatibilité non détectée dans le cas Madame Müller, échappe au système, ce qui complique et rend parfois impossible toute investigation sur les biens-fonds en possession d'une personne définie. Or, une telle information n'est pas sans importance dans le cadre d'une enquête où des délits ont été commis.

Sans l'utilisation d'un identificateur, l'identification univoque de personnes peut déboucher sur des erreurs et de faux appariements. Si l'on veut garantir dans les registres fonciers une identification univoque des personnes, il est indispensable de recourir à un identificateur univoque de personnes.

4.2.3 Travaux en cours et perspectives

Le message concernant la modification du Code civil suisse du 16 avril 2014 (Enregistrement de l'état civil et registre foncier) est actuellement à l'examen. Il n'a pas encore été traité au Parlement. La requête y est formulée de gérer le registre foncier au moyen du NAVS à 13 chiffres comme identificateur de personnes [15], avec pour objectif d'identifier de manière claire les propriétaires qui y figurent. Pour l'échange d'informations avec des services ou des organismes qui ne sont pas habilités à utiliser systématiquement le NAVS13, il est prévu d'utiliser un numéro d'identification personnel sectoriel, dérivant du NAVS13. Cet identifiant sectoriel dérivant du NAVS13 permettrait de ne pas divulguer le numéro AVS à 13 chiffres du propriétaire.

4.3 Cas de figure: l'Association des Services des Automobiles

4.3.1 Situation initiale et description du cas de figure

L'Association des Services des automobiles (Asa) est compétente, entre autres, en matière d'administration et d'enregistrement des cours de formation obligatoire pour nouveaux conducteurs, chauffeurs de poids lourds, moniteurs de conduite et camionneurs véhiculant des produits dangereux.

À la réception d'une autorisation de conduire, toutes ces personnes se voient attribuer un numéro d'identification FABER qu'elles conserveront toute leur vie et qui figure en impression sur leur permis de conduire. Ce numéro FABER est un identifiant qui figure dans le Registre des autorisations de conduire (FABER) géré par l'Office fédéral des routes (OFROU) et qui est établi pour toute personne qui fait une demande d'autorisation de conduire. On peut déduire l'étendue exacte de FABER en consultant l'art 3 de l'Ordonnance sur le Registre des autorisations de conduire [16].
Le numéro FABER sert d'identificateur univoque à l'Asa dans presque tous les cas. Mais à nouveau il existe des exceptions : certaines personnes n'ont pas forcément un permis de conduire, elles ne possèdent donc pas d'identifiant FABER. Ainsi, par exemple, les enseignants qui donnent les cours de formation ne disposent pas tous d'un permis de conduire et ne peuvent donc pas toujours être gérés par le biais d'un identifiant FABER.

En outre des efforts sont actuellement déployés pour que l'Asa gère désormais également les cours obligatoires de formation continue pour le personnel médical (médecins de famille et médecins des transports) et pour les psychologues. Là également se pose le problème que tout le monde, dans le domaine de la santé, ne possède pas forcément un permis de conduire. Certaines personnes n'auront donc pas d'identifiant FABER. Afin de disposer quand même d'un identificateur univoque dans ces cas-là, l'Office fédéral de la santé publique a trouvé un arrangement avec l'Asa autorisant celle-ci à utiliser le GLN (Global Location Number), anciennement code EAN. Il est possible que les cours de formation des secouristes soient désormais également gérés par l'Asa. Là aussi, certaines personnes (env. 20%) n'auront pas encore de permis de conduire en raison de leur jeune âge, et ne disposeront donc pas d'identifiant FABER. Pour cette catégorie de personnes, il n'existe actuellement aucun identificateur univoque de personnes, raison pour laquelle on serait contraint de recourir par exemple au NAVS13.

4.3.2 Conséquences d'une non-utilisation du NAVS13

Le cas étudié plus haut fait apparaître clairement que le numéro d'identification FABER n'empêche pas l'apparition récurrente d'exceptions où cet identificateur univoque ne peut pas être utilisé. En effet, seules les personnes qui possèdent un permis de conduire figurent dans le registre FABER (au cas où la personne déposerait son permis par la suite, le numéro d'identification FABER subsisterait jusqu'à son décès).
Lorsque des cas exceptionnels apparaissent, on essaie de se débrouiller en recourant à d'autres identifiants (en l'occurrence le GLN) qui, à leur tour, ne valent que pour un cercle limité de personnes. Pour certains cas exceptionnels, par exemple les enseignants sans permis de conduire, le seul recours possible est le NAVS13, car c'est le seul identificateur univoque que toutes les personnes de ce groupe possèdent en commun.

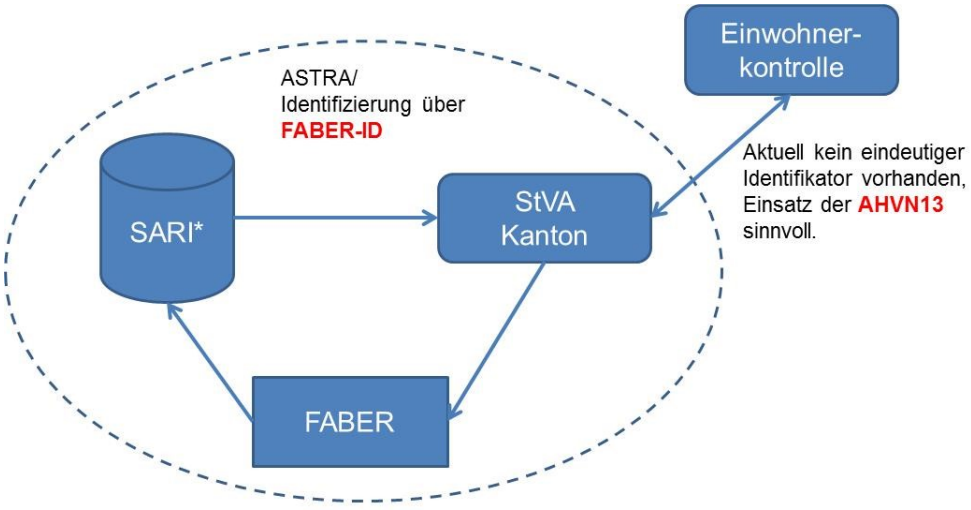
4.3.3 Travaux en cours et perspectives

Pour être en mesure d'utiliser un identificateur univoque et applicable d'une manière générale aux cas exceptionnels existants, l'Asa soutient l'introduction du numéro AVS à 13 chiffres comme identificateur de personnes uniforme et commun à toutes les organisations. En raison du coût élevé de cette mesure, l'identifiant FABER ne serait pas remplacé tout de suite par le NAVS13. Il est permis d'envisager un passage graduel, au fil des prochaines décennies.

4.4 Cas de figure: les Offices cantonaux de la circulation routière

4.4.1 Situation initiale et description du cas de figure

Les Offices cantonaux de la circulation routière et de la navigation (OCRN) se servent des données de l'Asa et utilisent donc ainsi le numéro d'identification FABER comme identificateur univoque. Pour l'établissement des taxes automobiles, par exemple, il est impératif pour les offices de la circulation routière de connaître l'adresse actuelle des détenteurs de véhicule. Comme ceux-ci omettent souvent de communiquer leur nouvelle adresse aux offices de la circulation routière lorsqu'ils déménagent, les OCRN obtiennent généralement ces changements d'adresse par le biais des Contrôles des habitants. Les OCRN transmettent les informations reçues au registre FABER. À l'Office fédéral des Routes, l'identification de la personne s'effectue au moyen du numéro d'identification FABER.



*System für Administration, Registrierung und Information

Illustration 4: Représentation de la possibilité d'utiliser le NAVS13 pour communiquer entre les Contrôles des habitants et les Offices cantonaux de la circulation routière

4.4.2 Conséquences d'une non-utilisation du NAVS13

Le numéro d'identification FABER est du ressort de l'Office fédéral des routes. Il ne peut être utilisé que par l'Asa et les Offices cantonaux de la circulation routière. C'est pourquoi, pour la mise en correspondance des bases de données entre les Offices cantonaux de la circulation routière et les Contrôles des habitants, on utilise les attributs suivants : nom, prénom, date de naissance. Si cette combinaison apparaît à diverses reprises, l'office cantonal des routes respectif doit vérifier manuellement de quelle personne il s'agit, occasionnant ainsi des frais récurrents qui ne peuvent être supprimés que par l'utilisation d'un NAVS13.

4.4.3 Travaux en cours et perspectives

L'introduction d'un NAVS13 pourrait simplifier la communication entre les Offices de la circulation routière et les Contrôles des habitants, dans la mesure où, grâce au numéro AVS à 13 chiffres, tout changement d'adresse pourrait être attribué aux personnes concernées. C'est la raison pour laquelle l'utilisation généralisée d'un NAVS13 dans un tel contexte est pertinente.

4.5 Cas de figure: la navigation

4.5.1 Situation initiale et description du cas de figure

Toutes les questions relatives à la navigation relèvent de la compétence de l'Office fédéral des transports (OFT). L'enregistrement des bateaux n'est pourtant pas géré par le biais de la Confédération, mais par les Offices cantonaux de la circulation routière. Chaque canton possède donc son propre registre des détenteurs de bateaux, avec chaque fois son propre identificateur univoque de personnes. En cas de déménagement d'un canton à l'autre, le détenteur de bateau reçoit chaque fois un nouvel identificateur.

4.5.2 L'introduction du NAVS13 : une chance à saisir

L'introduction d'un numéro AVS à 13 chiffres pourrait déboucher sur une gestion plus uniforme des données. L'utilisation du NAVS13 rendrait en effet superflue l'attribution d'un nouveau numéro d'identification et réduirait donc d'autant les frais administratifs. Un bel exemple de ces démarches coûteuses en temps et en argent, liées à la gestion cantonale de chaque dossier, nous est donné par l'accident survenu il y a quelques années sur le lac de Bienne. Là, il fallait identifier dans les plus brefs délais le détenteur d'un bateau bien précis; mais comme plusieurs cantons étaient impliqués, les démarches ont été longues et l'enquête a pris du retard.

4.5.3 Travaux en cours et perspectives

À l'heure actuelle, il n'y a pas de travaux prévus. Mais, comme nous l'avons démontré plus haut, l'utilisation du NAVS13 pourrait grandement faciliter les démarches.

4.6 Cas de figure : le casier judiciaire informatisé VOSTRA

4.6.1 Situation initiale et description du cas de figure

Conformément à l'Ordonnance sur le casier judiciaire, dite Ordonnance Vostra, le casier judiciaire informatisé VOSTRA (système entièrement automatisé) gère les jugements, les sanctions et les décisions judiciaires [17]. Actuellement, 700'000 personnes figurent dans ce système. La responsabilité de VOSTRA incombe à l'Office fédéral de la justice (OFJ). VOSTRA est géré et perfectionné en permanence par le Centre de services informatiques CSI-DFJP. Celui-ci procède chaque année à un release des données qui requiert 400 jours-personnes, sans compter les ressources externes auxquelles il faut faire appel. Pour assurer le bon fonctionnement du centre

et la qualité des données, l'OFJ emploie cinq personnes. Pour VOSTRA, le principal défi à relever est que, contrairement aux cas de figure précédents, les personnes enregistrées n'ont souvent aucun intérêt à être correctement identifiées. Concernant l'exactitude de l'identification des personnes, nous avons relevé deux cas de figure: celui où la personne doit être correctement identifiée par le biais d'une requête isolée et celui où il y a des recoupements avec d'autres systèmes (parfois des systèmes d'autres organisations) qui recourent à VOSTRA ou qui, en fonction des bases juridiques appropriées, ont également le droit d'y recourir et dépendent donc d'une connexion correcte.
Une loi fédérale concernant l'amélioration de l'échange d'informations entre les autorités au sujet des armes [18] est actuellement débattue au Conseil national. Cet objet propose une modification du code pénal qui permettrait un échange sûr, simple et univoque avec VOSTRA, en se basant sur le numéro AVS à 13 chiffres. Un tel échange de données pourrait se faire avec le Système d'information sur le personnel de l'armée (SIPA). Pour le recrutement et l'avancement de son personnel, l'Armée a en effet besoin d'extraits du casier judiciaire VOSTRA. Cet échange de données a lieu périodiquement et il est partiellement automatisé. D'autres points de recoupement, partiellement automatisés, existent également avec les justices pénales cantonales et les registres fédéraux (SYMIC, Infostar). Néanmoins, les données doivent être saisies à plusieurs reprises dans des systèmes différents. L'ajustement entre les systèmes s'effectue manuellement, et la commande d'un extrait de casier judiciaire s'effectue au moyen d'attributs personnels comme le nom de famille, le nom à la naissance, le prénom, la date de naissance, le nom et la date de naissance des parents. Cette procédure prend forcément beaucoup de temps et elle est source d'erreurs.

4.6.2 Conséquences d'une non-utilisation du NAVS13

Volontaire ou involontaire, une erreur d'identification dans VOSTRA peut avoir des conséquences d'une portée considérable. Ainsi, en indiquant de fausses informations, une personne peut fort bien, en fonction des circonstances, se faire délivrer indûment un extrait de casier judiciaire vierge. Réciproquement, une personne peut se voir remettre un extrait de casier judiciaire basé sur des données erronées. Il s'agit d'empêcher les deux cas de figure par une identification de personnes si possible efficace. L'identification basée sur les attributs personnels n'est pas suffisante, car ceux-ci ne font preuve d'aucune cohérence, peuvent être modifiés si les circonstances s'y prêtent, par exemple lors du mariage, ou ne peuvent pas être comparés parce que leurs formulations écrites diffèrent. L'univocité non plus n'est pas garantie dans tous les cas, même en utilisant plusieurs attributs personnels.

Il est difficile de chiffrer le coût administratif généré par le registre VOSTRA tel qu'il est géré aujourd'hui, à savoir sans unificateur de personnes uniforme et commun à toutes les organisations. Du côté du registre VOSTRA, plusieurs personnes sont employées à nettoyer les données et à effectuer des recherches en lien avec l'identification des personnes. Ces recherches consistent à consulter d'autres registres ou à prendre directement contact avec d'autres unités administratives, qui à leur tour devront consacrer davantage de temps et d'argent pour procéder, souvent manuellement, aux vérifications demandées.
L'échange d'informations au sein même de l'administration fédérale, avec les cantons et avec l'Armée est coûteux, source d'erreurs et prend du temps. Ce qui a pour conséquence que les vérifications aussi entraînent forcément des coûts élevés.
Les conséquences indirectes d'une attribution personnelle erronée excédaient le cadre de ce rapport et n'étaient pas mesurables avec les informations à disposition.

4.6.3 Travaux en cours et perspectives

La création d'une base légale permettant l'utilisation du NAVS13 a déjà été abordée dans le cadre du message 13.109 [18]. Pour introduire dans VOSTRA le numéro d'assuré AVS à 13 chiffres tel que le prévoit l'art. 50e de la LAVS, et pour programmer un recoupement entre PISA et VOSTRA, il faut compter sur un coût informatique d'env. 1,9 million de francs (estimation provisoire). Sont

notamment compris dans ce montant les coûts pour l'élaboration d'un concept de solution détaillé et les coûts des travaux de reprogrammation. L'actuelle infrastructure de VOSTRA a été développée en 2010. Son adaptation au NAVS13 occasionnerait un travail et des frais considérables, à tel point qu'aujourd'hui on se demande s'il vaut vraiment la peine de procéder à une telle adaptation et s'il ne serait pas préférable d'abandonner tout le système. Il n'existe pas encore d'estimation des coûts pour une refonte intégrale du système. Mais l'objectif (et les efforts de l'Office fédéral de la Justice le démontrent bien) demeure de simplifier les processus et d'introduire pour VOSTRA une identification sûre des personnes par le biais du NAVS13.

4.7 Synthèse des résultats

Dans tous les cas d'application étudiés plus haut il s'agit d'identifier des personnes de manière univoque. Ce n'est généralement pas la tâche principale définie par la loi, cela sert uniquement à attribuer les bonnes personnes à tel ou tel cas concret. L'identification ne s'effectue qu'avec les attributs personnels à disposition (nom, prénom, date de naissance, etc.) ou par le biais d'un numéro d'identification personnel. Dans tous les cas étudiés, ces données personnelles et ces identificateurs sont gérés dans un registre spécifique à chaque administration, parfois actualisés à grands frais, ou pas actualisés du tout. C'est ainsi qu'au sein de l'administration, des données figurent plusieurs fois dans des systèmes différents, où elles sont gérées de manière redondante. Pour procéder à une identification univoque, les attributs personnels ne sont adéquats que dans une certaine mesure. Ce sont surtout les situations où il y a des recoupements entre systèmes qui requièrent une identification univoque. En l'absence d'identificateur univoque de personnes, la collaboration par-delà les frontières des organisations est présentée partout comme excessivement lourde.

Le coût administratif d'une identification correcte incombe aussi bien au service directement concerné qu'aux organisations en aval. Il arrive souvent que l'attribution peu claire d'une personne nécessite une recherche d'informations auprès de différents services. Dans la plupart des cas de figure évoqués précédemment, cette démarche s'effectue à la main par le biais d'un employé. Or, ces recherches manuelles et la complexité même de l'identification en général font que la durée totale des processus est très longue. Et pour obtenir une identification correcte, on recueille souvent des informations (date de naissance, lieu d'origine, indications sur les parents, etc…) qui ne sont d'aucune utilité pour la résolution du cas spécifique.

L'utilisation du NAVS13 comme identificateur est donc saluée. On apprécie tout particulièrement sa large diffusion. Les cas de figure évoqués précédemment ont mis en place des solutions développées bien avant l'introduction du NAVS13. C'est pourquoi la non-utilisation du NAVS13 comme identificateur est rendue responsable de la situation actuelle et citée comme principale cause des problèmes rencontrés aujourd'hui dans l'échange des données et dans l'identification.

5 Législations étrangères

L'objet de ce projet consistait non seulement à analyser quelques cas de figure en Suisse, mais également à examiner la législation à l'étranger. Trois pays d'Europe ont été pris en considération, dans lesquels on a déjà introduit un identificateur de personnes uniforme et commun à toutes les organisations. Le choix s'est porté sur le Danemark, les Pays-Bas et l'Espagne, parce que les conditions cadre dans ces pays sont à peu près comparables à celles de la Suisse. Pour les trois pays, des interviews d'experts ont été réalisées par téléphone.

5.1 Le registre central des personnes (RCP) au Danemark

Les informations concernant la situation au Danemark proviennent de recherches sur Internet et de deux interviews, l'une avec Monsieur Carsten Grage, Directeur du RCP au Ministère danois de l'Intérieur, l'autre avec Monsieur Rasmus Theede, Président du Conseil pour la Sécurité numérique. Ce Conseil pour la Sécurité numérique existe depuis trois ans. Au début il a réuni dans ses rangs surtout des personnes issues de l'économie privée. Aujourd'hui, des institutions

publiques y sont également représentées. Ce conseil d'experts fait autorité au Danemark en matière de protection des données et de cyber-sécurité. Les médias s'adressent à lui pour toute question relative à ce sujet.

5.1.1 Infrastructure et utilisation de l'identificateur de personnes

Le registre

Le registre central des personnes (RCP) a été introduit au Danemark en 1968. L'autorité qui assure le bon fonctionnement du RCP a son siège au Ministère de l'Intérieur. La base légale du RCP réglemente sa finalité et les modalités de sa gestion (règles sur la manière de saisir les données et de procéder aux mutations, ainsi que les règles sur la communication des données à des tiers) [19]. Le registre contient les données de toutes les personnes domiciliées au Danemark, essentiellement les données personnelles de base suivantes:

- Le *Civil Registration Number* (numéro RCP)
- Le nom complet
- L'adresse actuelle
- La nationalité
- L'état civil
- La date de naissance
- La profession

Le RCP contient des données actuelles, mais les données anciennes sont sauvegardées, archivées et tenues à disposition. En raison de la diversité des sources de provenance, il peut arriver qu'une personne soit saisie deux fois. Mais il s'agit d'une occurrence marginale.

Les sources du registre

Les personnes domiciliées au Danemark doivent se faire enregistrer auprès de l'administration de leur lieu de domicile. Par conséquent les administrations locales et communales comptent parmi les principales sources du RCP. Les autres sources sont les églises, les hôpitaux et le Ministère de la justice. C'est ainsi que, par exemple, les naissances et les décès sont directement saisis dans le système par le biais de l'hôpital.

La communication des données

En principe, toutes les données qui figurent dans le RCP peuvent être communiquées à toutes les administrations. Avant de communiquer des données à une autorité, on procède à une vérification initiale. L'autorité qui fait la demande s'engage à respecter la loi sur la protection des données [20]. Les modalités de transfert des données sont alors établies. L'autorité qui fait la demande peut accéder à n'importe quelle information figurant dans le système RCP qui pourrait lui être utile dans l'exercice de son activité. Le respect de la protection des données est du ressort de la responsabilité de l'utilisateur des données.

La communication à des institutions privées de données figurant dans le RCP suit la même logique. L'entreprise s'engage à respecter la loi sur la protection des données et établit par contrat les modalités de transfert des données. La communication des données est autorisée dans la mesure où celles-ci peuvent faire état des indications suivantes:

- Nom et date de naissance; ou
- Nom et adresse; ou
- Nom et numéro RCP.

Après indication de ces caractéristiques personnelles, les données RCP peuvent être communiquées à l'entreprise concernée.

Les entreprises privées n'obtiennent du Registre central RCP que le nom et l'adresse de personnes qui n'ont fait aucune requête de protection de leurs données (voir paragraphe suivant). De même, les entreprises privées peuvent obtenir l'information du décès d'une personne ou de son souhait de ne pas être contactée à des fins de marketing. Une solution technique a été intégrée dans le système pour s'assurer que les entreprises privées n'obtiennent du RCP que ces informations-là, et rien d'autre.

Une personne peut exiger la protection de ses données. Les possibilités de protection suivantes sont prévues:

a) Protection contre la communication de données à des fins de marketing
b) Protection contre la communication de données à des fins de statistique ou de recherche
c) Protection contre la communication de données collectées pour être ensuite introduites dans des répertoires publics physiques
d) Protection contre la communication de données en général

Lorsqu'une personne demande une protection générale de ses données, conformément au point d), les données personnelles concernées ne sont pas communiquées à des entreprises privées durant une période d'une année. Cette requête peut être formulée sans justification. À l'heure actuelle, environ 40'000 à 50'000 personnes font usage de ce droit. La protection expire après une année et doit faire l'objet d'une nouvelle demande. Dans des cas particuliers, lorsque la demande est dûment motivée, cette protection peut être accordée pour plusieurs années. Cette clause de sauvegarde a été élargie le 1er mai 2014. Dans des cas spéciaux et sur la base d'une décision de la police, l'adresse actuelle d'une personne peut désormais être radiée du RCP. La protection décrite au point c) a perdu de son importance en raison de l'apparition des répertoires *online*. La protection décrite au point b) a été sollicitée par env. 800'000 personnes, à savoir 20% de la population globale. Afin de renforcer la pertinence de la statistique danoise, la possibilité de demander cette protection-là a été supprimée le 1er avril 2014, et la protection des 800'000 personnes concernées a été effacée.

Dans les services *online,* l'authentification s'effectue par le biais du NEM-ID. Il s'agit d'un système de mot de passe à usage unique (One-Time Password), qui est utilisé aussi bien pour l'utilisation de services *online* privés que publics. Pour l'enregistrement, le numéro RCP est obligatoire. Une fois enregistré(e), la détentrice ou le détenteur du NEM-ID reçoit un nouveau mot de passe lorsqu'elle (il) veut s'authentifier pour un service.

5.1.2 Utilité socio-économique de l'identificateur de personnes

Les avantages du système n'ont jamais été quantifiés. D'une manière générale, son utilité se manifeste par un gain d'efficacité énorme et par la qualité accrue des données, donc également par leur fiabilité dans le domaine des données personnelles. Le système est utilisé par l'intégralité du secteur public et la majeure partie du secteur privé. À l'heure actuelle, env. 32'000 utilisateurs disposent d'un accès direct à ce système, et chaque nuit il y a 340 extraits qui y sont effectués. Les gros clients du secteur privé sont les banques, les assurances, les fournisseurs de télécommunications et les avocat(e)s.

Rien n'illustre mieux la chaîne des transactions informatiques que les naissances et les décès. Les naissances sont directement saisies par la sage-femme dans le système RCP. Les informations parviennent donc aux autorités compétentes quelques minutes seulement après la naissance. S'appuyant sur ces informations, les parents peuvent, le lendemain déjà, introduire

une demande de prestations pour frais de garde et pour soins de santé. Les décès peuvent également être saisis directement dans le système depuis l'hôpital. La même nuit, l'information est transmise à toutes les bases de données reliées au système. Toutes les démarches indispensables en cas de décès, comme l'interruption des prestations de l'aide sociale, le blocage des comptes bancaires ou le versement d'une assurance-vie, peuvent être entreprises sans délai.

Le nombre de transactions informatiques est très élevé; il le serait tout autant sans RCP. L'avantage du système RCP est de ne générer ni nouvelles transactions, ni transactions supplémentaires. Le RCP ne fait qu'aider à rendre le déroulement de ces transactions plus efficace, à améliorer la qualité et la sécurité des données.

5.1.3 Le numéro RCP vu sous l'angle de la protection des données

L'utilité du système RCP fait l'objet dans la société danoise d'un consensus général. On peut débattre de la question si une autorité définie a le droit d'utiliser les données d'une autre autorité ou non. Mais c'est un débat qui doit être mené même en l'absence d'un système comme le RCP. Le système RCP n'est rien d'autre qu'une simplification de la communication des informations.

Le registre des personnes RCP ne contient guère de données sensibles. Le numéro RCP n'est qu'un attribut qui sert à l'identification univoque de personnes. Il n'est pas un moyen d'authentification: en clair, il ne donne pas le droit d'accéder à des données personnelles, par exemple du domaine de la santé ou des assurances sociales. Les personnes interviewées estiment à titre privé que le numéro RCP pourrait même être rendu public. À leur avis, ce numéro n'a pas en soi de valeur de protection.

Des mesures ont été prises pour garantir la protection des données, aussi bien sur le plan législatif que sur le plan technique. Techniquement, on a satisfait aux exigences en matière de sécurité selon le principe du *best practice*. Quant à la base légale, elle s'appuie sur deux lois: la loi sur le RCP et la loi sur la protection des données.

Le Conseil pour la sécurité numérique estime qu'il est aujourd'hui devenu nécessaire d'agir dans le domaine de la protection et de la sécurité des données [21]. Ce sont surtout les cas d'usurpation d'identité qui sont les plus préoccupants. Les petits délinquants s'approprient en effet les données d'une personne (y compris le numéro RCP) en les dérobant dans la boîte aux lettres. Ils utilisent ensuite ces informations pour percevoir des prestations ou exécuter des transactions informatiques au nom du titulaire du numéro. Autre préoccupation: l'utilisation du numéro RCP comme moyen d'authentification. Le jour où cette démarche est autorisée, il serait possible, uniquement sur indication du numéro RCP, d'accéder aux données personnelles du titulaire de ce numéro.

5.1.4 Recommandations à la Suisse

Le système danois a fait ses preuves et s'avère d'une grande efficacité dans les transactions informatiques entre les diverses autorités administratives. L'Estonie et d'autres pays de l'Europe de l'Est se sont inspirés de ce système après la Guerre froide. Tous les pays scandinaves disposent d'un système similaire. En Suède comme en Estonie, le numéro utilisé comme identificateur univoque est même accessible au public.

Afin de garantir la sécurité des données dans un contexte d'identificateur univoque de personnes, en l'occurrence le numéro RCP, il est recommandé de ne gérer dans le Registre central des personnes qu'un ensemble de données le plus restreint possible. Le mieux serait de ne pas conserver de données sensibles dans cette base de données. C'est une recommandation que fait également le Conseil pour la Sécurité numérique. Il est conseillé de conserver

séparément les données relatives à l'identité et les autres données. Les autres recommandations du Conseil pour la Sécurité numérique sont les suivantes :

- Adopter des règles claires en matière d'authentification;
- Laisser ouverte la possibilité de changer les numéros qui ont été attribués (par ex. en cas d'usurpation d'identité) ;
- Introduire un numéro non-parlant, c'est-à-dire ne pas utiliser un numéro qui permettrait de faire des déductions sur des données personnelles comme l'âge ou le sexe ;
- Utiliser les technologies dites *Privacy Impact Assessments*[4] et *Privacy Enhancing*.

5.2 Le Burger Service Nummer (BSN) aux Pays-Bas

Les informations concernant la situation aux Pays-Bas proviennent de recherches sur Internet et d'une interview téléphonique avec Monsieur Uijl Kees, chef du BSN au Ministère hollandais de l'Intérieur.

5.2.1 Infrastructure et utilisation de l'identificateur de personnes

Le registre

Le Burger Service Nummer *(BSN)* a été introduit en 2007 [22], en remplacement du numéro d'assurance sociale et d'identification fiscale (*SoFi number*). Aujourd'hui, la première saisie s'effectue au niveau communal. Toutes les personnes qui résident plus de quatre mois aux Pays-Bas doivent se faire enregistrer dans leur commune. Pour cela, elles doivent présenter un passeport valide, un certificat de naissance ainsi qu'une preuve qu'elles résident bien aux Pays-Bas. Les citoyens néerlandais résidant à l'étranger doivent effectuer la même démarche et disposer d'un BSN.

Le BSN figure en impression sur le passeport, la carte d'identité et le permis de conduire. Il s'agit d'un numéro personnel.

Les données personnelles ainsi recueillies sont tenues dans un registre central, le *Basisregistratie personen (BRP).*

Dans ce BRP figurent les données personnelles suivantes [23]:

- Nom, prénom, date de naissance, lieu de naissance, pays de naissance
- Informations sur les parents
- Informations sur les enfants
- État civil
- Nationalité, statut de séjour
- Adresse du domicile
- BSN

Les sources du registre [23]

Deux bases de données servent de sources principales au BSN: un registre qui contient des informations sur tous les ressortissants hollandais et un registre qui contient des informations sur tous les ressortissants étrangers résidant aux Pays-Bas.

Toute personne enregistrée peut demander la modification, la correction ou le complément de ses données auprès du Contrôle des habitants de sa commune. Pour la rectification de ses données, la personne doit se présenter personnellement au Contrôle des habitants, prouver son

[4] Un rapport d'évaluation, qui vérifie que les directives en matière de protection des données sont respectées et qui délivre des recommandations

identité et l'exactitude de son exigence, par ex. au moyen d'une attestation de domicile ou d'un certificat de mariage.

La communication des données [24]

Une base légale régit la communication du BSN dans le domaine public. Les autorités administratives qui, pour répondre au mandat que leur impose la loi, ont besoin de données figurant dans le registre central BRP, obtiennent ces données indispensables gratuitement. Les autorités en question sont, par exemple, l'administration fiscale, l'administration des douanes ou les services des assurances sociales. Depuis le 1er juin 2009, le BSN est exigé par la loi dans toute communication d'informations sur les patients ou les clients dans le domaine de la santé. Le numéro est également utilisé dans le domaine de la formation.

Toute utilisation du BSN dans le secteur privé nécessite une base légale.

Si on en fait la demande, il est possible d'empêcher la communication de ses données personnelles à des entreprises et à des privés.

5.2.2 Utilité socio-économique de l'identificateur de personnes

Le BSN est perçu comme un élément incontournable qui augmente la qualité des services publics. Il permet un échange d'informations fiable, efficace et légal entre les diverses autorités administratives. De plus, il permet la saisie unique de données utiles dans les administrations publiques. Autorisée par la loi, la communication de ces données entre les diverses autorités est ainsi grandement facilitée, voire réduite.

5.2.3 Le registre vu sous l'angle de la protection des données

La lutte contre l'usurpation d'identité est explicitement mentionnée comme l'une des raisons qui a conduit à l'introduction du BSN. Sur ce point, l'introduction de ce numéro est donc plutôt perçue comme une mesure visant à *renforcer* la protection des données. La loi interdit formellement aux titulaires d'un numéro BSN de le communiquer plus loin. Il s'agit d'un numéro personnel qu'il convient de protéger [22].

Les bases légales garantissant la protection des données dans le cadre de l'utilisation du BSN sont : la Loi sur le BRP et la Loi sur la protection des données.

Pour tout échange légal d'informations entre autorités administratives, l'utilisation du BSN est obligatoire, ce qui augmente la fiabilité et la qualité des données.

5.3 Le registre du Documento Nacional de Identidad (DNI) en Espagne

Les informations concernant la situation en Espagne proviennent de recherches sur Internet et d'une interview avec Monsieur Carlos Gómez Muñoz, chef de *l'Electronic Identification Unit* à la Direction informatique du Ministère espagnol des Finances et de l'Administration publique.

5.3.1 Infrastructure et utilisation de l'identificateur de personnes

Le registre

En Espagne, c'est le numéro de la carte d'identité (Documento Nacional de Identidad DNI) qui fait office d'identificateur de personnes. Cette carte et le registre correspondant ont été introduits en 1944 et régulièrement implémentés par la suite. La carte a fait l'objet de diverses modifications; elle a notamment été équipée de fonctions électroniques.
C'est la police espagnole qui est habilitée à gérer ce registre. Les bases légales pour la DNI fixent la finalité et la gestion du registre (règles sur la saisie des données, sur les transactions

informatiques et sur la communication des données à des tiers). En Espagne, la possession d'une carte DNI est obligatoire pour tous les citoyens espagnols de plus de 14 ans domiciliés dans le pays. Avant 14 ans il est possible d'obtenir une carte d'identité à titre facultatif.

Dans la DDNI figurent les données personnelles suivantes [25], communes à tous les Espagnols de plus de 14 ans domiciliés dans le pays:

- Numéro DNI
- Nom complet
- Adresse actuelle
- État civil
- Date de naissance
- Nationalité
- Lieu de naissance
- Nom des parents

Le numéro personnel sert également de numéro d'identification fiscale (*Número de Identificación Fiscal NIF)* ; il figure aussi sur le permis de conduire. Les ressortissants étrangers reçoivent leur propre numéro d'identification fiscale (*Número de Identidad de Extranjero*). Comme le numéro ne saisit les citoyens espagnols qu'à partir de leur quatorzième année, les assurances sociales et le domaine de la santé utilisent des identifiants spécifiques à leur secteur.

Les sources du registre

Les personnes résidant en Espagne doivent se faire enregistrer auprès de l'autorité administrative de leur lieu de domicile. Les informations issues de cet enregistrement doivent ensuite être transmises à la police. Les changements d'adresse peuvent s'effectuer *online*, dans la mesure où la police peut accéder aux données relatives à l'adresse par le biais du registre de la statistique, à qui tout changement d'adresse est communiqué par les autorités locales.

La communication des données

En principe, toutes les données figurant dans le registre DNI peuvent être communiquées à toutes les autorités administratives. Après avoir passé par un processus administratif initial, l'autorité obtient, par le biais d'un service broker, les données personnelles qui figurent dans le registre DNI, à la condition que le citoyen concerné consente à ce que ses données personnelles soient utilisées, ou alors qu'il existe une base légale autorisant la sortie de ces données (par ex. soupçon de fraude).

Le numéro de carte d'identité DIN est saisi et utilisé comme identificateur secondaire par de nombreux privés. Mais les privés n'ont pas accès au registre public. Pour les paris en ligne, par exemple, le fournisseur privé obtiendra au moyen du DNI une vérification de l'âge, mais aucune autre donnée personnelle.

5.3.2 Utilité socio-économique de l'identificateur de personnes

Les avantages du système n'ont jamais été quantifiés, car l'identificateur est à la disposition de l'administration déjà depuis le début de l'informatisation. On lui reconnaît pour principaux avantages son efficacité dans l'échange de données entre diverses autorités administratives (par ex. en cas de déménagement dans une autre province) et la bonne qualité des données. Mais comme l'identificateur de personnes se limite aux ressortissants espagnols de plus de 14 ans, il s'ensuit qu'il est nécessaire de recourir à d'autres identificateurs. Pour simplifier les processus, il a été décidé d'établir un identificateur de personnes dès la naissance. Ce processus est

actuellement en cours d'implémentation. Le numéro de carte DNI pourra ensuite dériver de cet identificateur de personnes.

5.3.3 Le numéro DNI vu sous l'angle de la protection des données

En raison de sa longue histoire, l'utilisation du numéro DIN est bien ancrée dans la population. Le recours à un numéro d'identification ne pose pas de problème particulier pour la protection des données. La législation stipule que les citoyens sont propriétaires de leurs données et que celles-ci n'ont pas le droit d'être communiquées sans leur assentiment. Indépendamment de l'identificateur, l'utilisation de ces informations par diverses collectes de données n'est donc pas autorisée sans le consentement du titulaire du numéro.
Les administrations publiques qui utilisent le DNI s'engagent à garantir la sécurité des données et à ne pas accepter le numéro comme seul et unique moyen d'authentification.

5.3.4 Recommandations à la Suisse

La perception du numéro par les citoyens est décisive. En Espagne, le système a fait ses preuves ; il est perçu comme utile et d'usage facile. Il n'a débouché sur aucune mauvaise expérience. Le fait qu'on ne puisse pas utiliser les données sans le consentement des citoyens, instaure un climat de confiance.

5.4 Récapitulation

Les trois exemples tirés de l'espace européen montrent que l'utilisation que l'on fait d'un utilisateur univoque de personnes diffère considérablement d'un pays à l'autre. Le contexte historique est également très différent. Tandis que les Pays-Bas utilisent un identificateur de personnes très récent (le BSN est en activité depuis 2007), le RCP au Danemark existe depuis bientôt 50 ans, et le DNI en Espagne même depuis plus de 70 ans. Dans les trois pays, seules sont enregistrées dans le registre les données personnelles de base les plus importantes. Dans chacun des trois cas, le registre ne contient donc que peu (voire pas) de données sensibles, ce qui garantit une certaine sécurité des données. Pour l'instant (mais une modification est d'ores et déjà envisagée) l'Espagne limite son identificateur univoque de personnes aux citoyens espagnols à partir de l'âge de 14 ans. En revanche, au Danemark et en Hollande l'identificateur univoque de personnes est utilisé pour toutes les personnes domiciliées dans le pays, indépendamment de leur nationalité. La complexité des systèmes en jeu varie parfois énormément d'un pays à l'autre. Ainsi, au Danemark il y a différentes sources de données (autorités administratives, églises, hôpitaux et Ministère de la justice), tandis qu'aux Pays-Bas et en Espagne, les sources des données se limitent aux autorités administratives.

Les trois pays ont ceci en commun qu'ils perçoivent tous l'utilisation d'un identificateur univoque comme quelque chose de très utile qui contribue grandement à l'efficacité de l'administration. Certes, les personnes interviewées au Danemark et en Espagne ont mis le doigt sur les risques d'usurpation d'identité. Mais il est intéressant de relever que la personne interviewée en Hollande considère au contraire l'identificateur univoque comme le meilleur moyen de lutter contre l'usurpation d'identité.

Pour la Suisse, la leçon à tirer de ces exemples est que l'utilisation d'un identificateur univoque de personnes serait d'une grande utilité pour accroître l'efficacité de l'administration. Chacun des trois registres étudiés se limite aux données personnelles de base les plus importantes. La protection des données et la cyber-sécurité sont certes des thèmes essentiels, qui gagnent d'ailleurs en importance. Mais ils ne s'opposent nullement à l'introduction d'un identificateur de personnes.

Avant d'introduire un identificateur de personnes, il importe surtout, comme dans les trois pays étudiés, de créer la base légale et les réglementations qui permettent d'utiliser sans risques un identificateur de personnes.

En guise de conclusion, on peut dire que l'identificateur univoque de personnes est utilisé fort différemment d'un pays à l'autre, mais que sa contribution à l'amélioration de l'efficacité au sein de l'administration est un atout incontestable.

6 Analyse et considérations générales

Dans ce chapitre, nous livrerons une analyse des résultats issus de l'étude à la fois des cas de figure et des législations étrangères, et nous procéderons à des considérations générales. Dans un premier temps, nous comparerons les systèmes en vigueur à l'étranger (dans les trois pays considérés) au système NAVS13 en vigueur en Suisse. Ensuite nous analyserons les diverses manières d'aborder le problème de la protection des données, et nous relèverons les différences existant entre les cas de figure évoqués en Suisse et les situations à l'étranger. Dans un deuxième temps, nous mettrons à nouveau l'accent sur la Suisse. Nous considérerons globalement les risques et les coûts qui résultent de la situation actuelle, et nous livrerons une synthèse de notre analyse.

6.1 Comparaison avec l'étranger

Les interviews avec les experts à l'étranger montrent que l'utilisation d'un identificateur univoque de personnes à l'échelle nationale est compatible avec la protection des données. L'utilisation de ce numéro est toujours intégrée dans un système qui est constitué d'un registre central de données personnelles et qui repose principalement sur deux lois: une loi régissant la gestion du registre et une loi sur la protection des données. L'illustration 5 montre un modèle avec les bases de données intégrées dans le système (en bleu) et les bases légales correspondantes (en vert). La loi sur la tenue des registres réglemente quelles données peuvent être gérées dans le registre, quand une mutation est autorisée, à qui et dans quelles conditions les données peuvent être transmises. Elle fixe également quand la communication des données est interdite en raison de la protection des données.

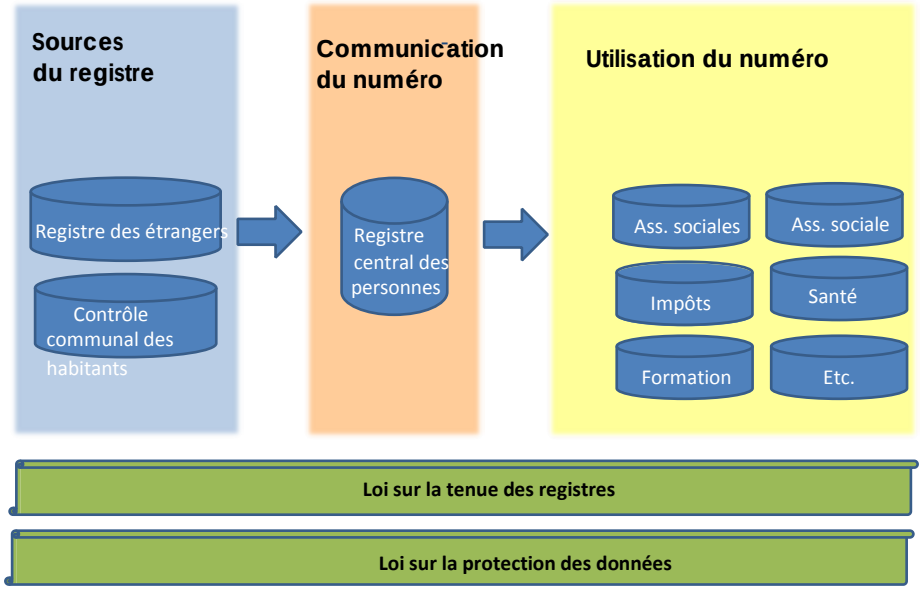


Illustration 5: représentation modélisée des systèmes d'identification des personnes à l'étranger (Source: graphique élaboré par nos soins)

Bases légales

La différence est manifeste: elle réside dans le nombre de lois sur lesquelles repose ce système (à comparer avec le graphique 1, au chapitre 3.4), tout particulièrement en ce qui concerne la communication des données. Dans les trois pays européens qui ont fait l'objet de notre étude, la saisie, la gestion et l'utilisation des données personnelles par le biais de l'identificateur de personnes sont réglementées à l'aide de deux lois. De son côté, la Suisse compte déjà deux lois rien que pour la tenue du registre et une multitude d'autres lois pour l'utilisation des données[5].

Infrastructure

Tandis que dans les trois pays européens étudiés la communication des numéros s'effectue par un registre central des personnes, en Suisse l'état civil est géré par les registres d'état civil et centralisé dans Infostar. Mais ce sont les mêmes données personnelles qui figurent dans la base de données UPI et dans Infostar ; cette distinction perd donc toute pertinence. En Suisse comme dans les trois pays étudiés, l'autorité habilitée à utiliser les données est aussi celle qui gère le numéro univoque.

Autorités habilitées à utiliser les données

Les Pays-Bas, l'Espagne et le Danemark ont ceci en commun qu'ils permettent tous trois à toutes les autorités administratives d'utiliser l'identificateur univoque de personnes, pour autant que ces autorités en aient besoin pour remplir un mandat légal. L'utilisation des données par des institutions de l'économie privée n'est autorisée qu'au Danemark sans base légale supplémentaire, avec néanmoins la possibilité laissée aux personnes concernées de l'interdire. Ici aussi, la différence avec la Suisse est manifeste. En Suisse, chaque utilisation du NAVS13 requiert une base légale séparée, même si sa nécessité est déjà fixée dans une loi spécifique.

Protection des données

Dans les bases légales des trois pays étudiés, il est chaque fois stipulé que toute utilisation doit respecter les directives en matière de protection des données. C'est la raison pour laquelle la Loi sur la tenue des registres renvoie systématiquement à la Loi sur la protection des données. À l'étranger, dans les trois pays étudiés on veille à ce qu'une autorité n'obtienne que les données dont elle a besoin pour remplir son mandat légal. En pratique, il est chaque fois procédé à un examen initial. Parfois un accord est conclu, aux termes duquel l'utilisateur s'engage à garantir la protection de ces données. À la différence de la Suisse, l'utilisation en soi d'un identificateur univoque de personnes n'est pas perçue comme une menace pour la protection des données.

Réserves concernant la sécurité

À la différence de la Suisse, l'appariement inapproprié de données n'est pas considéré comme un gros danger, car chaque utilisation par une autorité administrative est systématiquement légitimée par la législation correspondante. Cette opinion est partagée même par le Conseil danois pour la Sécurité numérique, un conseil d'experts indépendants qui milite pour la protection et la sécurité des données dans la société numérique. Ce même conseil émet par contre des réserves concernant la sécurité, même si ces réserves se réfèrent essentiellement aux problèmes d'usurpation d'identité.

Recommandations à la Suisse

Les experts consultés se montrent unanimes: l'utilisation d'un identificateur univoque de personnes à l'échelle nationale accroîtrait considérablement l'efficacité des procédures administratives et la qualité des données. Ils n'émettent aucune réserve à l'introduction d'un tel identifiant. Concrètement, ils ont formulé les recommandations suivantes :

[5] Dans le cadre de cette expertise, il n'a pas été possible d'établir une liste exhaustive des lois qui permettent l'utilisation systématique du NAVS13. Pour atteindre un tel objectif, il faudrait procéder à un examen de toutes les lois fédérales et de toutes les lois cantonales.

- *Utiliser les technologies dites privacy enhancing [6] / privacy by design[7]*
- *Séparer physiquement les données d'identité des autres données*
- *N'utiliser le numéro que pour l'identification univoque d'une personne, non comme moyen d'authentification*
- *Établir des directives d'authentification strictes - Encourager l'utilisation de privacy risk assessments.*

Les experts consultés recommandent également de recourir à un numéro non-parlant et de saisir l'intégralité de la population domiciliée dans le pays. Ces deux éléments ont déjà été mis en place dans le NAVS13.

6.2 Implication sur la protection des données

Les expériences menées à l'étranger montrent que l'utilisation d'un identificateur univoque de personnes à l'échelle nationale peut être compatible avec la protection des données. Les dangers esquissés par le Préposé fédéral à la protection des données et à la transparence (PFPDT) concernent les appariements illicites d'ensembles de données personnelles et la création illicite de profils personnels. On entend régulièrement l'argument que la simple utilisation du NAVS13 dans les différents registres comportant des données personnelles constitue déjà en soi un affaiblissement de la protection des données. Mais cette argumentation ne résiste pas à l'analyse.

Avoir connaissance d'un identificateur ne signifie pas avoir accès aux données qui se trouvent derrière

Les arguments exposés par les représentants de la protection des données impliquent de manière répétée que la simple connaissance du NAVS13 permet d'accéder aux données sensibles qui lui sont liées ou qui se trouvent derrière, et qui méritent d'être protégées. Cette déduction n'est pas exacte. Si elle l'était, les attributs identifiants univoques devraient également et automatiquement ouvrir l'accès au reste des données personnelles qui leur sont liées. Dans la question de l'accès aux données, il faut faire la distinction entre l'acte d'identifier, l'acte d'authentifier et l'acte d'autoriser.

Par analogie, imaginons la situation suivante: l'adresse du domicile privé d'une personne est un identificateur pour l'endroit où cette personne possède une partie de sa propriété privée. Mais avoir connaissance de l'adresse du domicile privé n'autorise pas et ne rend pas non plus possible l'accès aux données de la propriété privée qui lui sont liées.

Afin que seules des personnes habilitées puissent accéder à des données sensibles sur des tiers (données qui méritent donc d'être protégées), chaque source de données requiert une solution appropriée pour gérer l'identité et les accès de chaque utilisateur (en anglais : *Identity and Access Management*, IAM). Pour les registres contenant des données personnelles, il ne faut pas qu'un tel système IAM utilise l'identificateur univoque de personnes comme attribut pour authentifier un accès à des données méritant protection. Par conséquent, il ne suffit pas qu'une personne ait connaissance du numéro d'identification univoque d'une autre personne pour que cela l'autorise automatiquement à accéder aux données de cette autre personne.

Il y a des appariements de données à l'intérieur du cadre légal, avec ou sans NAVS13.

Les cas de figure étudiés dans la présente expertise et les expériences menées à l'étranger mettent en évidence les appariements de données exigés pour répondre aux besoins d'un mandat légal. La nécessité d'un appariement résulte des opérations quotidiennes que doivent effectuer les administrations publiques, par exemple celles de la Police, de la Justice et de

[6] Un set d'outils, d'applications et de mécanismes informatiques, *resp* un set de mesures informatiques qui sont intégrés dans les services online et dans les applications métier et qui permettent de protéger les données liées à des informations sur les personnes à l'intérieur de ces services ou de ces applications métier.

[7] Dans le domaine de l'ingénierie des systèmes, approche qui tient compte de la protection des données tout au long du processus d'élaboration.

l'Armée. Dans ces cas-là, les appariements entre ensembles de données sont donc autorisés par la loi et nécessaires à l'accomplissement de mandats imposés par loi. Ils sont également faisables sans NAVS13, ce que démontre la pratique actuelle. Ainsi, qu'il y ait un appariement de données personnelles à l'intérieur ou à l'extérieur du cadre juridique, n'a aucun lien avec le caractère utilisable du NAVS13. Lorsqu'un employé de l'administration accède de manière illicite à des données personnelles dans différents registres et établit ainsi un profil de manière illégitime, cet employé peut le faire avec ou sans NAVS13. On ne voit pas pourquoi l'utilisation générale du NAVS13 dans les divers registres de la fonction publique aurait pour conséquence d'engendrer obligatoirement ou automatiquement une recrudescence d'accès illicites aux données personnelles. L'appariement des données personnelles doit continuer d'être soumis (même en cas d'utilisation du NAVS13) à des obligations légales strictes, dont l'observation doit être imposée et surveillée par l'État.
Bien que l'appariement de données soit permis, voire indispensable, dans les faits on ne parvient souvent pas à établir des appariements, parce qu'il n'y a pas d'identificateur de personnes, comme le montrent les cas de figure étudiés. Il en résulte pour les administrations, mais aussi pour les privés, un préjudice qui serait facilement évitable avec un identificateur de personnes.

La non-utilisation du NAVS13 affaiblit la protection des données
Comme le montrent les cas de figure étudiés, la non-utilisation du NAVS13 nécessite dans divers domaines de recourir à des solutions alternatives qui permettent de relier entre eux les ensembles de données personnelles, de les ajuster ou de les transférer. Comme le numéro AVS à 13 chiffres ne peut pas être utilisé, dans certains cas on crée un identificateur *ad hoc*, qui est utilisé de manière inter-organisationnelle sur la base de règlements locaux d'utilisation des registres et des données. Là où des ensembles de données personnelles doivent être appariés entre divers registres, l'identification des personnes s'effectue par le biais d'une comparaison d'un nombre varié d'attributs identifiants. Même si de tels appariements de données personnelles, qui ont déjà cours aujourd'hui, sont des actions irréprochables sur le plan juridique, ils obligent à recourir, pour les appliquer, à des solutions de contournement qui occasionnent des coûts évitables et comportent un risque marqué d'erreur d'identification. Or, comme nous l'avons vu dans les cas de figure étudiés, ces erreurs d'identification débouchent forcément sur des atteintes à la protection des données, parce que les données de la personne mal identifiée sont consultées, appariées et transmises.

L'utilisation du NAVS13 dans les registres de l'administration publique renforce la protection des données

Les dangers liés à l'absence d'un identificateur univoque de personnes ont fait l'objet d'une description minutieuse dans l'analyse des cas de figure. Ils sont résumés dans le tableau 1, au chapitre 6.3.

L'utilisation du NAVS13 dans les registres permettrait de réduire considérablement les identifications erronées lors de démarches légales effectuées par l'administration publique. Dans les situations d'urgence, les ensembles de données personnelles enregistrées de manière décentralisée peuvent en effet être identifiés plus rapidement. En cas d'usurpation d'identité, la fraude est discernable plus rapidement et avec plus de précision, pour autant que le système soit équipé d'une plateforme IAM appropriée avec un login d'accès en conséquence.
En outre, la possibilité que donne le NAVS13 de relier entre elles des données personnelles permettrait beaucoup plus facilement aux administrations qui détiennent des données, d'octroyer ou non des informations soumises au droit sur la protection des données (Art. 8 LPD)). De cette façon, elles pourraient révéler de manière simple, rapide et surtout complète, de quelles informations elles disposent sur la personne qui opère la requête. De même les ensembles de données relatives aux autorisations d'exploitation (qui a le droit d'utiliser quelles données et comment) seraient beaucoup plus faciles à vérifier que ce n'est le cas aujourd'hui sans identificateur uniforme de personnes. Pour appuyer l'obligation d'information et le contrôle, la

tenue d'un répertoire de métadonnées des informations en lien avec le NAVS13 serait un puissant auxiliaire pour mettre en place une protection des données globale.

Voilà pour tout ce qui est susceptible de renforcer la protection des données.

En réponse à l'expertise Biaggini (2002), on peut donc avancer qu'il y a un intérêt public à utiliser le NAVS13 comme identificateur de personnes uniforme et commun à toutes les organisations, car celui-ci renforcerait la protection des données.

6.3 Risques de la non-utilisation d'un identificateur univoque de personnes en Suisse

Dans ce chapitre on trouvera en résumé et sous forme de synthèse les risques d'une non-utilisation du NAVS13 tels qu'ils ont été évoqués dans les cas de figure. Le tableau 1 répertorie tous les cas de figure abordés et connus.

Cas de figure	Usage	Gestion à l'heure actuelle	Risque dans la procédure actuelle
VOSTRA	Dans le cadre militaire, vérifier la bonne réputation d'une personne avant de procéder à son recrutement ou à son avancement.	Identification manuelle au moyen des attributs personnels.	Ferreur d'identification d'une personne.
VOSTRA	Dans le cadre d'un mandat légal, améliorer l'échange d'informations entre deux autorités administratives (notamment dans la gestion des armes à feu).	Ajustement manuel entre les systèmes au niveau fédéral; soutien partiel par le biais des recoupements.	Erreur d'identification d'une personne.
VOSTRA	Vérifier les antécédents judiciaires d'une personne dans les processus de naturalisation.	Requêtes individuelles dans le registre VOSTRA.	Erreur d'identification d'une personne.
VOSTRA	Établir les extraits de casier judiciaire.	Requêtes individuelles dans le registre VOSTRA.	En raison d'une erreur d'identification, remise d'un faux extrait de casier et atteinte à la protection des données, car divulgation d'informations confidentielles concernant une autre personne.
Assujettissement à la Taxe sur la Valeur ajoutée	Examiner le risque, c'est-à-dire vérifier si la personne a encore des factures de TVA impayées en relation avec d'autres entreprises.	Investigations manuelles par un employé.	Risque indéterminé; les postes non soldés restent non soldés, sans conséquences pour le débiteur.
Remboursement de l'impôt anticipé des ressortissants étrangers.	Examiner le risque, c'est-à-dire vérifier s'il y a des factures d'impôts impayées avant de procéder au remboursement.	Investigations manuelles par un employé.	Risque indéterminé; malgré la présence possible de postes non soldés, le montant est versé.
Asa	Administrer les membres du corps enseignant en charge des cours de formation de l'Asa.	L'identifiant FABER ID est utilisé pour les personnes détentrices d'un permis de conduire. Il est nécessaire de recourir au NAVS13 pour les personnes sans permis de conduire.	Impossibilité d'identifier les membres du corps enseignant non-titulaires d'un permis de conduire.

Asa	Identifier les médecins qui participent aux cours obligatoires de formation continue et qui n'ont pas de permis de conduire.	L'identifiant FABER ID est utilisé pour les personnes détentrices d'un permis de conduire. Le numéro GLN est utilisé pour les personnes sans permis de conduire.	Pas de risque, mais coûts supplémentaires, car plusieurs identifications.
Offices cantonaux de la circulation routière et de la navigation (OCRN)	Améliorer la communication entre les OCRN et les Contrôles des habitants.	Traitement manuel	Envoi de la taxe automobile à de fausses adresses.
Offices cantonaux de la circulation routière et de la navigation (OCRN)	Instaurer un identificateur uniforme pour les détenteurs de bateaux.	Chaque canton attribue son propre identificateur	En cas d'accident, la qualité de détenteur du véhicule est très difficile, voire impossible à établir.
VOSTRA	Extrait spécial du casier judiciaire destiné à des privés. (Registre des pédophiles)	Identification manuelle au moyen de plusieurs attributs.	Erreur d'identification, inculpation de la fausse personne avec des conséquences qui mettent sa vie en péril
Registre des Poursuites (Arrondissements)	Extrait du registre des poursuites	Identification manuelle au moyen de plusieurs attributs.	Erreur d'identification, Obtention frauduleuse d'extraits du registre des poursuites concernant autrui.
Registre des Poursuites (Arrondissements)	Extrait du registre des poursuites	Identification manuelle au moyen de plusieurs attributs.	Erreur d'identification. Harcèlement en engageant des poursuites contre de personnes non impliquées.
Registre du commerce (Arrondissements)	Extrait du registre du commerce en matière pénale	Identification manuelle au moyen de plusieurs attributs.	Erreur d'identification
Registre foncier	Gel des capitaux	Identification manuelle au moyen de plusieurs attributs.	Erreur d'identification, gel des capitaux de fausses personnes, impossibilité de détecter une fortune en cas d'héritage ou en matière pénale.

Tableau 1: Risques dans les procédures actuelles

Le tableau ci-dessus affiche 15 cas de figure. Dans trois d'entre eux, on utilise déjà un identificateur de personnes. Dans tous les autres, l'identification des personnes s'effectue manuellement.

Dans tous les cas, les autorités administratives sont fortement entravées dans l'accomplissement de leur mandat légal. Dans neuf cas, la non-utilisation du NAVS13 entraîne un risque d'erreur d'identification. Ce risque peut avoir de graves conséquences pour les personnes concernées, victimes tantôt d'atteintes à la protection des données, tantôt même d'accusations fallacieuses. Dans quatre cas, l'identification est quasiment impossible sans l'utilisation d'un identificateur de personnes. Dans ces cas-là, l'état demeure en grande partie dans le flou, surtout dans le cadre des investigations liées au gel des capitaux.

Mais même dans les cas où l'on utilise déjà un identificateur de personnes, les problèmes d'identification de personnes subsistent. Ainsi l'identifiant FABER ID n'attribuera un numéro qu'aux personnes détentrices d'un permis de conduire. Les démarches administratives qui

utilisent comme identificateur de personnes le numéro d'identification FABER ID, se heurtent à des limites dès qu'elles :

- doivent saisir dans leur système des personnes qui n'ont pas de permis de conduire;
- ont besoin d'informations de la part d'autorités qui gèrent un registre autre que le FABER ID.

6.4 Estimation des coûts

L'estimation des coûts s'avère une entreprise difficile, en raison de nombreuses inconnues. Les coûts actuels dans les divers domaines ne permettent pas de dégager une affectation claire des dépenses occasionnées par le travail d'identification. Soit parce que celles-ci sont englobées dans d'autres dépenses, soit parce qu'elles n'existent pas dans les faits, étant donné qu'une identification est presque impossible dans le système actuel. Même une estimation des coûts futurs s'avère difficile, car d'une situation initiale à l'autre, ces coûts peuvent varier fortement. C'est pourquoi ce chapitre ne propose qu'une ébauche possible d'examen des coûts.

Estimation des coûts dans la perspective d'une administration.

Les coûts découlent des systèmes nécessaires (conception, implémentation, exploitation, maintenance), des données (saisie, ajustement, entretien), des processus (identification, ajustement, collecte) et de la législation. Pour une analyse globale des coûts, nous sommes partis de la situation actuelle. Ces coûts se composent des exigences en matière de compliance (lois), des dépenses liées aux processus (notamment identification des personnes, durée des processus), de l'administration des données (notamment leur saisie et leur entretien) et des infrastructures informatiques utilisées à l'heure actuelle (exploitation, support). Le projet d'introduire le NAVS13 comme identificateur univoque de personnes implique des coûts pour adapter les systèmes et les processus. Il faut s'attendre à des dépenses indispensables pour l'adaptation des processus, des données (migrations, ajustements, collectes), des infrastructures informatiques (conception, implémentation) et de la législation. L'objectif d'une telle reconversion, c'est que les coûts d'exploitation dans la situation future soient moins élevés que dans la situation actuelle, c'est-à-dire qu'avec le temps on puisse économiser les dépenses occasionnées par la migration des données.

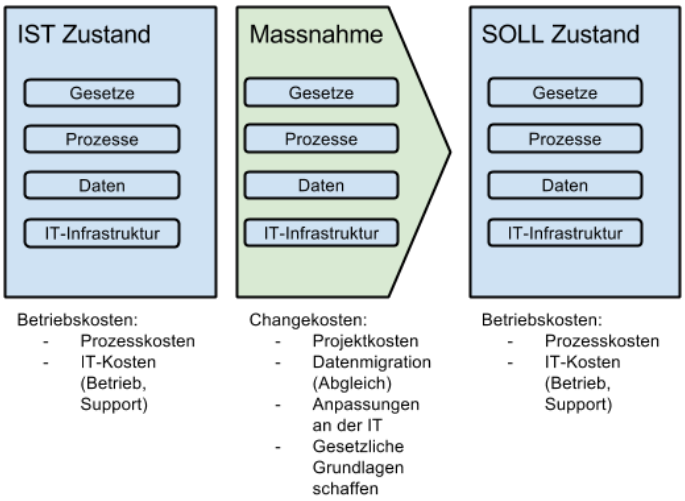


Illustration 6: analyse des coûts dans la perspective d'une administration

Selon une estimation provisoire des coûts, l'introduction du NAVS13 dans le casier judiciaire informatisé VOSTRA (cas étudié au chapitre 4.6), avec les adaptations au système qui en résulteraient, reviendrait à env. 1,9 million de francs. Les coûts actuels en personnel sont estimés à env. 400'000 francs. Mais il n'existe pas d'autres estimations connues des coûts.

Coûts dans une perspective économique globale

Pour introduire un identificateur uniforme de personnes, on peut envisager trois types de solution:

1. Type A: des registres qui auraient le droit de gérer le NAVS13 comme identificateur de personnes (Utilisation directe du NAVS13)
2. Type B : des registres qui auraient le droit de dériver des identificateurs à partir du NAVS13 et de les utiliser de manière sectorielle (Utilisation indirecte du NAVS13)
3. Type C : des registres qui gèrent leurs propres identificateurs, sans aucune corrélation avec le NAVS13 (Non-utilisation du NAVS13)

Le tableau 2 illustre les coûts engendrés par chaque solution au niveau suisse

Sur le plan suisse, à quelques rares secteurs près, chaque registre gère aujourd'hui pour lui ses propres identificateurs (cf. type C sur le tableau 2). Les registres qui ne peuvent pas recourir au NAVS13 comme identificateur univoque de personnes ou qui ont le droit d'utiliser des identificateurs qui dérivent du NAVS13, sont contraints de concevoir leurs propres solutions pour identifier les personnes, puis de les implémenter, de les exploiter et de les entretenir (cf. types B et C, sur le tableau 2). En règle générale, cela signifie également qu'ils doivent recueillir et entretenir les données permettant d'identifier ces personnes. On sait par expérience que ces processus exigent un travail considérable, sont difficiles à maîtriser et sujets à l'erreur. Mais comme le montrent les cas de figure étudiés, cette situation est actuellement la norme en Suisse, à tous les niveaux fédéraux.

Les registres qui ont le droit de recourir au NAVS13 comme identificateur univoque de personnes, ont besoin pour cela d'une base égale (cf. type A dans le tableau 2). Cette base doit être créée individuellement pour chaque cas d'usage, aussi bien au niveau fédéral qu'au niveau de chaque canton. Les coûts concrets qu'occasionnerait la création en Suisse d'une législation aux divers niveaux fédéraux ne sont pas connus pour l'instant. Mais selon l'avis de certains experts, ils devraient s'élever chaque fois à « plusieurs personnes/années », c'est-à-dire approximativement à un million de francs pour chaque loi.

La non-utilisation d'un identificateur de personnes occasionne chaque jour des coûts qui sont engendrés par les processus de longue durée nécessaires à l'identification, à l'ajustement à la collecte des données.

- Identification: les données personnelles qui figurent dans les différents registres doivent pouvoir être attribuées aux bonnes personnes. Là où les identificateurs respectifs ne sont pas connus vers l'extérieur (ce qui est la norme pour les registres qui disposent d'identificateurs autonomes), il est impératif que la personne réelle soit ajustée à l'ensemble des données personnelles qui font l'objet de la requête sur la base d'attributs identifiants univoques. Dans de nombreux cas, un processus manuel est nécessaire (cf. cas de figure, par ex. parce que le nom est mal orthographié). De tels processus d'identification se déroulent mille fois par jour en Suisse. D'une part l'application des processus (tout particulièrement lorsqu'ils sont manuels) requiert beaucoup de personnel, donc s'avère onéreux. D'autre part les conséquences liées aux erreurs d'identification (qui sont inévitables surtout lorsque les processus sont manuels) peuvent être très graves et occasionner des coûts supplémentaires par des processus en aval.
- Ajustement & collecte: dans les différents registres, les ensembles de données personnelles doivent régulièrement être ajustés les uns aux autres ; en partie il est également nécessaire de procéder à des transferts ou à des regroupements dans d'autres registres. Là aussi le problème de l'identification refait surface, avec à nouveau pour conséquence des processus d'ajustement dispendieux, parfois à effectuer manuellement. Lorsque des données personnelles initialement de qualité douteuse ont été transférées

d'un registre à un autre, il en résulte ensuite inévitablement des processus de nettoyage très coûteux. Et en Suisse, ces coûts surviennent chaque année des milliers de fois.

Le tableau 2 montre que le nombre des dépenses résultant d'une non-utilisation du NAVS13 est supérieur au nombre de dépenses résultant de son utilisation. Bien que le montant effectif de ces coûts dépende chaque fois du nombre de transactions et de la quantité de données gérées dans tel ou tel registre (par ex. uniquement les détenteurs de véhicules au lieu de la population suisse tout entière), il s'agit de tenir compte du fait que les coûts globaux figurant dans le tableau 2 sont à chaque fois encourus plusieurs fois. Ils sont en effet générés lors de chaque utilisation, directe ou indirecte, du NAVS13, et chaque fois qu'un identificateur de personnes indépendant du NAVS13 est créé dans un secteur. Sur ce point, les coûts globaux qui figurent sur le tableau 2 doivent donc être multipliés par le nombre d'utilisations/ le nombre de secteurs. Tandis que, dans le cas de solutions dérivées (type B) il y a encore un grand nombre de personnes saisies dans des systèmes communs, avec des données entretenues dans des systèmes communs, les dépenses encourues dans le troisième type de cas (type C) doivent être multipliées par des dizaines de fois. Si l'on considère que le type C est actuellement le système majoritairement en vigueur en Suisse, on peut sans autre avancer que la Suisse pratique aujourd'hui la solution la plus coûteuse qui soit.

Coûts encourus / dépenses	Type de coût	Coûts encourus utilisation directe (Type A)	Coûts encourus utilisation indirecte (Type B)	Coûts encourus Non-utilisation (Type C)
Établissement d'une base légale	Introduction d'un système des coûts	√	√	
Établissement d'un registre de personnes pour l'attribution des numéros				√
Nettoyage et migration des données (ajustement)		√	√	√
Adaptations informatiques dans les registres concernés		√	√	√
Notification des nouveaux numéros aux titulaires des numéros			√	√
Dépenses informatiques courantes pour l'exploitation du registre des personnes, *resp.* des numéros	Exploitation courante des coûts		√	√
Affectation courante des numéros (nouvelle saisie de données)			√	√
Garantie de la qualité et de l'actualité des données existantes (mutation des données lors des modifications de no, etc.			√	(√)[8]

[8] Pour abaisser les coûts, on renonce souvent à sécuriser l'actualité et la qualité des données gérées dans le registre.

Coût encourus dans les registres concernés pour l'ajustement courant des données avec le registre des numéros		√	(√)[9]	(√)[10]
Coûts dans leur globalité		Chaque nouvelle utilisation systématique entraîne des coûts pour l'établissement d'une base légale et pour le rattachement au système existant.	Les coûts liés à la création et à la gestion d'un registre des numéros tombent. Néanmoins chaque nouvelle utilisation entraîne des coûts pour l'attribution et l'entretien des numéros sectoriels dérivés.	L'établissement d'identificateurs autonomes requiert une réplication du système NAVS13 adaptée à la branche. Le montant des coûts dépend de la masse des données et du nombre des transactions gérés dans le système répliqué.

Tableau 2: coûts dans une perspective économique globale

Pour conclure, il est permis de constater que, jusqu'à présent, ces coûts encourus en permanence à travers toute la Suisse ne sont pas facturés. Généralement, les factures relatives à ces coûts (par exemple les analyses d'impact sur la réglementation) s'arrêtent au niveau des dépenses initiales et des charges d'exploitation liées aux systèmes d'identification des personnes. Mais les coûts engendrés par l'absence d'un identificateur de personnes, qui sont des coûts récurrents et en grande partie évitables, demeurent cachés à ce jour. De même, il n'y a aucune transparence sur les coûts encourus par les réglementations spéciales sur l'utilisation du NAVS13 au niveau de la Confédération et au niveau des 26 cantons. Si l'on prend pour référence les coûts connus engendrés par l'introduction et l'exploitation de l'UPI, il est permis d'avancer que l'utilisation généralisée à l'échelle suisse du NAVS13 dans tous les registres publics permettrait probablement de réaliser des économies potentielles sur les coûts à hauteur de centaines de millions de francs par année.

7 Conclusion

La Suisse dispose déjà d'un identificateur univoque de personnes à l'échelle nationale. Comme nous l'avons montré dans le chapitre 6.1, l'infrastructure qui existe à l'heure actuelle autour du NAVS13 est comparable à celle que l'on trouve à l'étranger dans les systèmes nationaux d'identification des personnes. Le système suisse peut même être qualifié d'avant-gardiste, parce qu'il gère un numéro qui ne permet aucune déduction sur la personne titulaire du numéro. C'est aussi un numéro qui englobe l'intégralité de la population résidant en Suisse depuis la naissance ou l'entrée dans le pays.

[9] L'existence ou non de ces coûts dépend du type d'utilisation du numéro.

[10] Ces coûts tombent pour les registres qui ne sont pas en relation avec d'autres registres.

La Suisse a besoin d'un identificateur de personnes uniforme et commun à toutes les organisations.
Le chapitre 6.3 montre non seulement que l'absence d'un identificateur univoque de personnes complique énormément les procédures administratives, mais aussi qu'elle comporte des risques considérables. Ainsi, les autorités administratives sont souvent fortement entravées dans l'accomplissement de leurs tâches légales, et des personnes subissent potentiellement des préjudices alors qu'elles ne sont pas concernées.

Identificateur univoque de personnes à l'échelle nationale, le NAVS13 a l'avantage d'exister déjà aujourd'hui. Son utilisation doit impérativement être prise en considération. À lui seul, le nombre de cas qui ont été relevés dans le cadre de cette expertise, indique que le besoin d'un identificateur univoque de personnes est une nécessité générale. Surtout si l'on songe que l'utilisation des identificateurs sectoriels de personnes atteint rapidement ses limites.

Les cas de figure étudiés dans cette expertise illustrent que, selon les cas, l'absence d'un identificateur univoque de personnes peut aussi avoir pour conséquence de porter atteinte à la protection des données. Ainsi, l'intérêt public dont parle l'expertise Biaggini (2002) ne passe pas uniquement par une meilleure qualité des données et une amélioration de leur efficacité, mais également par la nécessité générale d'éliminer les risques inhérents à la situation actuelle (notamment concernant la protection des données).

L'examen global des cas de figure montre également que l'unique alternative à l'utilisation du NAVS13 consiste à créer un identificateur sectoriel de personnes. Mais comme l'illustrent les cas de figure tirés du domaine de la circulation routière, les systèmes basés sur un identificateur sectoriel de personnes atteignent vite leurs limites. En l'absence d'alternative, les diverses autorités administratives s'efforcent séparément de créer les bases légales qui leur permettent d'utiliser systématiquement le NAVS13. Cette simple constatation répond d'ailleurs au critère de nécessité, exigence qui ressortait de l'expertise Biaggini (2002).

L'utilisation d'un identificateur de personnes uniforme et commun à toutes les organisations est parfaitement compatible avec la protection des données.
Les débats qui ont cours en Suisse ne font pas la distinction entre identification, authentification, et autorisation. Un identificateur univoque sert à identifier une personne de manière univoque, lorsque d'autres caractéristiques personnelles font défaut. Comme toutes les autres données personnelles, l'identificateur de personnes ne devrait être considéré que comme une caractéristique de plus, qu'il importe de protéger. La particularité de cette caractéristique personnelle, c'est qu'elle est attribuée par l'État.

Quant aux données, il s'agit de les sécuriser dans tous les processus numériques au moyen d'un système adéquat d'autorisation administrative et en recourant aux privacy enhancing technologies. Les expériences faites à l'étranger montrent que les Privacy Risk Assessments sont un bon moyen d'assurer la protection des données dans les processus administratifs. Les Privacy Risk Assesments contiennent des recommandations comment développer au mieux une infrastructure informatique et des processus permettant de procéder à des appariements de données bien définies, tout en satisfaisant aux directives sur la protection des données. L'autorisation d'accéder aux données doit être clairement réglementée et elle ne doit pas s'appuyer uniquement sur le numéro utilisé comme identificateur univoque de personnes. Pour conclure, il est à remarquer que ces mesures de protection sont indispensables même sans utilisation d'un identificateur de personnes uniforme et commun à toutes les organisations.

Si l'on applique les mesures de sécurité mentionnées précédemment, l'utilisation d'un identificateur de personnes uniforme et commun à toutes les organisations est même de nature à renforcer la protection des données. Comme on le voit dans les cas de figure étudiés, les atteintes à la protection des données qui surviennent aujourd'hui pourraient être évitées, et pour une administration ce serait un jeu d'enfant de donner à une personne des informations sur les données qu'elle détient à son sujet et qu'elle utilise.

La situation actuelle n'est pas satisfaisante
Les risques évoqués et les importants coûts annuels encourus réclament une solution rapide qui aborde le problème de manière globale, non de manière sectorielle. Bien que de très nombreux domaines se trouvent confrontés au même problème, chacun d'entre eux doit aujourd'hui mettre en place une solution individuelle pour chaque problème. Pour la Suisse dans son ensemble, il en résulte chaque fois des coûts importants, car chaque fois il s'agit de créer une base légale et, parfois, de créer un registre des personnes pour attribuer un identificateur à une partie de la population, puis de l'entretenir (par ex. personnes détentrices de permis de conduire).

Pour la Suisse, il vaudrait la peine d'utiliser le NAVS13 comme identificateur uniforme de personnes à l'échelle nationale dans toutes les administrations publiques, d'autant plus que le NAVS13 exploite déjà l'infrastructure appropriée et que le besoin d'un identificateur de personnes se fait sentir dans de nombreux domaines. Mais si l'on prend en considération l'utilisation du NAVS13 comme identificateur univoque de personnes à l'échelle nationale, il ne suffira pas de modifier la base légale dans ce sens. Il s'agira de concevoir un système global susceptible de prendre en compte sérieusement et dès le début les dangers qui menacent la protection des données, un système qui intègre une configuration à la fois légale, technique et organisationnelle.

En regard des obligations internationales de la Suisse, les critères de ce numéro doivent faire l'objet d'un accord international. En effet, dans le cadre de l'échange automatique d'informations, ce n'est pas seulement l'identification des personnes résidant en Suisse qui est en jeu : celle de ressortissants étrangers qui ne résident pas en Suisse est également tout à fait pertinente. Inversement, dans le cadre de cet accord, il faut aussi que les autorités étrangères puissent identifier des ressortissants suisses au moyen d'un numéro univoque.

8 Recommandations

Il est donc recommandé à la Suisse d'aborder de manière globale les problèmes étudiés dans cette expertise, d'établir un concept global « d'identificateur uniforme de personnes à l'échelle nationale », qui placerait au centre de ses priorités la protection des données personnelles, tiendrait compte du système existant du NAVS13 et prendrait en considération à la fois les aspects légaux, techniques et organisationnels.

Il lui est également recommandé d'associer, déjà dans la phase d'initialisation, le Préposé fédéral à la protection des données (conformément à Hermes 5.1). Il convient également de coordonner les démarches avec les projets actuellement en marche à l'échelle nationale visant à introduire un justificatif d'identité électronique à l'échelle nationale (eID) [26] et avec la Fédération suisse d'identités (FSI) [27]. Il s'agit également de suivre de près les développements liés au postulat 12.3361 de la Commission des Institutions politiques du Conseil national relatif à l'échange de données d'adresses entre les registres des Contrôles des habitants, la poste et d'autres titulaires de données [28].

Enfin, il s'agira également de tenir compte des développements et des exigences liés au contexte international.

9 Table des illustrations

10 Sommaire des tableaux

11 Table des abréviations

Abréviation	Signification
AFC	Administration fédérale des Contributions
Asa	Association des Services des Automobiles
AVS	Assurance vieillesse et survivants
AVS13	Numéro d'assuré AVS à 13 chiffres
BRP	*Basisregistratie personen* (Registre central des personnes)
BSN	*Bürger service nummer* (Citizen Service Number)
CdC	Centrale de Compensation
CDF	Contrôle fédéral des Finances
CSI	Conférence suisse sur l'Informatique
CSI-DFJP	Centre de Services informatiques du Département fédéral de Justice et Police
DNI	*Documento Nacional de Identidad* (Numéro de carte d'identité)
FABER	Registre automatisé des autorisations de conduire
GLN	Global Location Number (anciennement code EAN)
HESB	Haute École spécialisée bernoise
IDE	Numéro d'identification des entreprises
Infostar	Registre fédéral de l'État civil
LAVS	Loi fédérale sur l'Assurance vieillesse et survivants
LHR	Loi fédérale sur l'Harmonisation des registres des habitants et d'autres registres officiels de personnes

LPP	Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité
NIF	*Número de Identificación Fiscal* (Numéro d'identification fiscale)
OCA	Ordonnance sur la carte d'assuré pour l'Assurance obligatoire des soins
OCRN	Office de la Circulation routière et de la Navigation
OFAS	Office fédéral des Assurances sociales
OFJ	Office fédéral de la Justice
OFROU	Office fédéral des Routes
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la Santé publique
PFPDT	Préposé fédéral à la Protection des données et à la Transparence
RCP	Registre central danois des personnes (*Det Centrale Personenregister*)
SARI	Système d'administration, d'enregistrement et d'information
SIPA	Système d'Information sur le Personnel de l'Armée
SoFi number	Aux Pays-Bas, numéro d'Assurance sociale et d'identification fiscale
SYMIC	Système d'Information central sur la Migration
TVA	Taxe sur la Valeur ajoutée
UPI	Unique Person Identification
VOSTRA	Casier judiciaire entièrement automatisé

12 Bibliographie

[1] Centrale de Compensation CdC, « Le numéro AVS à 13 chiffres (NAVS13) dans les assurances sociales fédérales » [Online]. Available: http://www.zas.admin.ch/org/00721/00722/index.html?lang=de. [Consulté le 19 06 2015].

[2] Centrale de Compensation CdC, « UPI » [Online]. Available: http://www.zas.admin.ch/org/00721/00758/index.html?lang=de. [Consulté le 19 06 2015].

[3] Centrale de Compensation CdC, (NAH/REY), « UPI – Manuel utilisateur (handbook). Version 1.04 », 21 novembre 2012. [Online]. Available: http://www.zas.admin.ch/org/00721/00758/00904/index.html?lang=de. [Consulté le 19 06 2015].

[4] Office fédéral des Assurances sociales OFAS, « Utilisation du NAVS13. Cahier des charges. Version 1.2 », 21 novembre 2012. [Online]. Available: http://www.zas.admin.ch/org/00721/00722/00896/index.html?lang=de. [consulté le 19 06 2015].

[5] Office fédéral de la Statistique OFS, « Harmonisation de registres officiels des personnes. Catalogue officiel des caractères », 2014. [Online]. Available:

http://www.bfs.admin.ch/bfs/portal/de/index/news/publikationen.html?publicationID=5567 . [Consulté le 19 06 2015].

[6] Centrale de Compensation CdC, « Utilisation systématique du NAVS13 », 16 avril 2015. [Online]. Available: http://www.zas.admin.ch/org/00721/00722/00901/index.html?lang=de. [Consulté le 19 06 2015].

[7] Conseil fédéral, « Ordonnance sur la carte d'assuré pour l'Assurance obligatoire des soins » (OCA)», 1er janvier 2009. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20062093/200901010000/832.105.pdf. [Consulté le 01 06 2015].

[8] G. Biaggini, « Expertise relative à un identificateur de personnes sous l'angle de la protection de la personnalité prévue dans le droit constitutionnel (Art. 13 CF). Avis de droit », [Online]. Available: http://www.edoeb.admin.ch/datenschutz/00786/00946/00949/index.html?lang=de. [Consulté le 26 06 2015].

[9] Préposé fédéral à la Protection des données et à la Transparence PFPDT, « Numéro AVS », [Online]. Available: http://www.edoeb.admin.ch/datenschutz/00786/00946/index.html?lang=de. [Consulté le 26 06 2015].

[10] Préposé fédéral à la Protection des données et à la Transparence PFPDT, « Contre la propagation du numéro d'assuré AVS », 16 avril 2014. [Online]. Available: http://www.edoeb.admin.ch/datenschutz/00786/00946/index.html?lang=de. [Consulté le 30 06 2015].

[11] Administration fédérale des Contributions (AFC), « Division principale de la TVA » [Online]. Available: http://www.estv.admin.ch/mwst/org/00338/00344/00353/index.html?lang=de. [Consulté le 30 06 2015].

[12] Contrôle fédéral des Finances CDF, «11391 ESTV Organisation und Instrumente der Betrugserkennung und Betrugsbekämpfung im Bereich Mehrwertsteuer».

[13] Office fédéral de la Justice OFJ, « Caractéristiques du Registre foncier », [Online]. Available: https://www.bj.admin.ch/bj/de/home/wirtschaft/grundbuch/merkmale.html. [Consulté le 25 06 2015].

[14] Office fédéral de la Justice OFJ, « Modèles de données eGris », [Online]. Available: https://www.bj.admin.ch/bj/de/home/wirtschaft/grundbuch/datenmodelle.html. [Consulté le 02 07 2015].

[15] Conseil fédéral, « Message concernant la modification du code civil », (Enregistrement de l'état civil et registre foncier) du 16 avril 2014 [Online]. Available: https://www.admin.ch/opc/de/federal-gazette/2014/3551.pdf. [Consulté le 25 06 2015].

[16] Conseil fédéral, « Ordonnance sur le registre des autorisations de conduire »,» 1er octobre 2011. [Online]. Available: https://www.admin.ch/opc/de/classifiedcompilation/20001349/index.html. [Consulté le 22 juin 2015].

[17] Conseil fédéral, « 311 Ordonnance sur le casier judiciaire (Ordonnance VOSTRA) » 01 janvier 2015. [Online]. Available: https://www.admin.ch/opc/de/classifiedcompilation/20061863/index.html. [Consulté en juin 2015].

[18] Conseil fédéral, « Message du 13 décembre 2013 relatif à la Loi fédérale concernant l'amélioration de l'échange d'informations entre les autorités au sujet des armes - 13.109 », 13 décembre 2013. [Online]. Available: https://www.admin.ch/opc/de/federal-gazette/2014/303.pdf. [consulté en juin 2015].

[19] Social Security Administration (GlobalDenmark Translations), « Executive Order on the Civil Registration System Act », Juli 2013. [Online]. Available: https://cpr.dk/media/163624/lovbekendtg_relse_eng_12070213.pdf. [Consulté le 15 06 2015].

[20] The Danish Data Protection Agency, « Compiled version of the Act on Processing of Personal Data », décembre 2012. [Online]. Available: http://www.datatilsynet.dk/english/the-act-onprocessing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-theact-on-processing-of-personal-data/. [Consulté le 15 06 2015].

[21] Rådet for Digital Sikkerhed, « Digital sikkerhed i Danmark 2014. Årsrapport fra Rådet for Digital Sikkerhed », mars 2015. [Online]. Available: http://digitalsikkerhed.dk/nyheder/nyhederfraraadet/nyhed/article/419/. [Consulté le 15 06 2015].

[22] Government of the Netherlands, « Identification documents. The Citizen Service Number (BSN) », [Online]. Available: http://www.government.nl/issues/identification-documents/the-citizenservice-number. [Consulté le 24 06 2015].

[23] Government of Netherlands, « Identification documents. The Municipal Personal Records Database », [Online]. Available: http://www.government.nl/issues/identification-documents/themunicipal-personal-records-database. [Consulté le 24 06 2015].

[24] Rijksdienst voor Identiteisgegevens. Ministerie van Binnenlandse Zaken en Koningkrijksrelaties, « BSN », [Online]. Available: http://www.rijksdienstvooridentiteitsgegevens.nl/BSN/Vraag_en_antwoord/Wetgeving. [Consulté le 24 06 2015].

[25] MINISTERIO DEL INTERIOR. Dirección General de la Policía., « Descripción del DNI electrónico », [Online]. Available: http://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_103&id_menu=[1]. [Consulté le 24 06 2015].

[26] Office fédéral de la Justice OFJ, «Consultation informelle – Identification électronique », 08 07 2015.
[Online]. Available: https://www.fedpol.admin.ch/fedpol/de/home/pass--identitaetskarte/pass_idk/ausweise.html. [Consulté le 04 08 2015].

[27] E-Government Suisse, « Services d'identification et de gestion des droits d'accès des participants à la cyberadministration B2.06 »,
[Online]. Available: http://www.egovernment.ch/b206/index.html?lang=en. [Consulté le 04 08 2015].

[28] Conseil fédéral, « Échange de données personnelles entre les registres des habitants, la Poste et d'autres détenteurs de données. Rapport du Conseil fédéral en réponse au postulat 12.3661 de la Commission des Institutions politiques du Conseil National du 16 août 2012 », 12 novembre 2014.
[Online]. Available: http://www.parlament.ch/sites/doc/CuriaFolgeseite/2012/20123661/Bericht%20BR%20D.pdf. Consulté le 04 08 2015].

[29] Conseil fédéral, « Message concernant une modification de la Loi fédérale sur l'assurance-vieillesse et survivants (Nouveau numéro d'assuré AVS) », 23 11 2005. [Online]. Available: https://www.admin.ch/opc/de/federal-gazette/2006/501.pdf. [Consulté le 04 08 2015].

[30] Chancellerie fédérale, « https:// https://www.ch.ch/fr/mariage-et-nom/ » 2015. [Online]. Available: https://www.ch.ch/de/heiraten-namenswahl/. [Consulté en juin 2015].

[31] P. Kummer, «Rapport final. Projet « Numéro d'assuré (NAVS13) comme identificateur de personne ». Harmonisation des registres », Office fédéral de la statistique OFS, Neuchâtel, 2010.

Annexe 1: liste des personnes interviewées

Liste des personnes interviewées

Patrick Riesen, Administration fédérale des Contributions AFC, chef du programme Fiscal-IT

Urs Paul Holenstein, Office fédéral de la Justice OFJ, directeur secteur de l'informatique juridique

Christian Buetler, Office fédéral de la Justice OFJ, Gestionnaire en applications du projet E-Government

Sven Britschgi, Association des Services des Automobiles Asa, administrateur

Christine Madl, Office fédéral de la Justice OFJ, responsable des applications VOSTRA et chef de projet informatique

Carsten Grage, Danish Ministry of Interior, CPR Office, Head of Division

Rasmus Theede, Danish independent Council of Digital Security, Chairman

Uijl Kees, Ministry of the Interior and Kingdom Relations, Citizenship and Information Directorate, Department of Identity, Policy Advisor

Carlos Gómez Muñoz, Ministry of Finance and Public Administration, ICT Civil Servant

Liste des personnes consultées

Thomas Steimer, Office fédéral de la Justice OFJ, Gestionnaire en applications de projet (Expert infostar)

Jérôme Magnin, Centralede Compensation CdC, chef de la section statistique et registre central

Patrick Kummer, Office fédéral de la Statistique OFS, section registre, chef de la section Bâtiments et Appartements

Annexe 2: Lignes directrices pour l'interview Cas de figure

Introduction

En Suisse, il n'existe pas d'identificateur de personnes uniforme et commun à toutes les organisations. L'utilisation de l'identificateur le plus répandu, le NAVS13, exige une base légale pour chaque utilisateur. Il résulte de cette situation des contraintes opérationnelles et des risques par manque d'univocité lors du traitement des données inter-organisationnelles. Jusqu'à présent, l'introduction d'identificateurs de personnes uniformes et communs à toutes les organisations a été empêchée par des considérations sur la protection des données. Les débats autour de la protection des données entravent la recherche de meilleures solutions et ignorent le fait que la non-utilisation du numéro AVS à 13 chiffres comporte elle-même de grands risques et suppose des occasions manquées.

La Haute École spécialisée bernoise HESB a été mandatée par la Conférence suisse sur l'Informatique CSI pour établir une expertise sur le thème du NAVS13 comme identificateur de personnes uniforme et commun à toutes les organisations. L'expertise examine notamment la question suivante: « Que risquons-nous et qu'est-ce que ça coûte de renoncer à utiliser un identificateur uniforme et commun à toutes les organisations? ». Par le biais de ces interviews, nous soulevons les problèmes qui sont déjà survenus jusqu'à présent, et qui résultent de la non-utilisation d'un identificateur uniforme et commun à toutes les organisations. Et nous examinons, dans les domaines actuels où un identificateur uniforme et commun à toutes les organisations a déjà été introduit, quels en sont les avantages.

Ces interviews montrent la perspective de l'organisation, mais ils n'en sont pas représentatifs : elles n'engagent que la personne qui effectue la déclaration.

Les questions de l'interview

Question d'introduction: Quel est, dans votre domaine d'activité, le principal besoin lié à l'identification des personnes? Comment cette identification est-elle effectuée actuellement ?

1. Connaissez-vous des exemples concrets qui ont entraîné un préjudice/des dépenses, parce qu'une personne n'a pas été identifiée correctement ?
2. Connaissez-vous des cas de figure ou des exemples de procédures/d'applications qui ne sont pas réalisables par manque d'un identificateur univoque de personnes ?
3. À quelle fréquence les cas évoqués dans les deux premières questions surviennent-ils? (par année, dans votre canton, en Suisse)
4. Pouvez-vous décrire les conséquences financières et non financières qui en résultent?
5. Dans quels cas procède-t-on à des appariements de données, et dans lesquels de ces cas l'utilisation du NAVS13 comme identificateur de personnes uniforme et commun à toutes les organisations serait-elle souhaitable ?
6. Comment les données personnelles sont-elles appariées aujourd'hui, et quels problèmes cela soulève-t-il ?
7. Quelles contraintes et quels coûts pourrait-on globalement économiser en utilisant le NAVS13 comme identificateur de personnes uniforme et commun à toutes les organisations ?
8. Est-ce qu'actuellement vous vous efforcez à créer une base légale permettant l'utilisation du NAVS13 comme identificateur de personnes?
    a. Si oui, quel est votre objectif? À combien estimez-vous les dépenses encourues?
    b. Si non, pourquoi ?

Question pour conclure: Êtes-vous favorable à l'utilisation du NAVS13 comme identificateur de personnes uniforme et commun à toutes les organisations ?

Annexe 3: Interview Guide NL

Introduction

Switzerland has no unique personal identifier. The use of the most common identifier of AHVN13 (the Swiss social security number) requires a legal basis for each application. This leads to operational challenges in data processing, especially in the case of cross-organizational or cross-sectoral data processing. The introduction of a unique personal identifier has been hitherto prevented by privacy concerns. The debate has until now ignored the great dangers related to identification and data processing in state agencies. The multiplicity of special regulations allowing the use of the AHVN13 at federal, as well as at cantonal level, hinders to overview how and for which purpose the number is actually used.

The Bern University of Applied Sciences has received a mandate by the Swiss Information Technology Union[17] to provide a report, illustrating the risks and the costs arising due to the absence of a unique identifier in e-government processes. The report should also discuss the experiences made by other countries in using such an identifier, especially for cross-organizational and cross-sectoral use. Special interest is given to particular provisions aimed at securing privacy. The latter shall be investigated in 2-3 short semi-structured interviews with experts.

Objectives of this interview:

- Get an idea of the net value of having a national unique personal identifier.
- Get insights on experiences made related to privacy issues ever since the introduction of the national unique personal identifier.
- Get knowledge on provisions installed or to be installed to secure privacy.

In the Netherlands the Citizen Service Number (BSN) has been introduced in 2007. It replaces the social security number and tax number (SoFi number). The SoFi number has been cancelled with effect from 6 January 2014. From this date on, all inhabitants must be registered at a municipality. The BSN is recorded in the Municipal Records Database (GBA) and is written on each person's passport, ID-card and driving license. Citizen Service numbers are also used to exchange patient information reliably and securely in the Electronic Patient Records Database (EPD). Since 1 June 2009, all care providers, needs assessment agencies and health insurers have had to refer to citizen service numbers when exchanging information about patients or clients. It is also used in the education sector.

In this respect, Switzerland would like to learn from the experiences of the Netherlands on their introduction of the BSN.

Interview Questions

1. Is the situation in the Netherlands as described above accurate?
2. Which processes and infrastructures have been cut after the introduction of the BSN (economic value)?
3. What values and benefits have been generated due to the introduction of the BSN (societal, cultural value)?
4. What have been main privacy concerns before the introduction of the BSN (identity theft, profiling, other)? Have any of the concerns been proven true? If yes, what were the consequences?
5. What provisions have been installed to secure privacy (legal technical, organizational)?

17 Assembly of cantonal ICT representatives

6. Based on your country's experiences, what recommendations would you give in order to secure the successful transformation of a social security number into a personal identifier?

Note
If approved by the interviewee, the phone call will be recorded for documentation purpose.

To be defined with interviewee at the beginning or end of the interview.

Follow Up
To be discussed directly after the interview.

Annexe 4: Interview Guide DK

Introduction

Switzerland has no unique personal identifier. The use of the most common identifier of AHVN13 (the Swiss social security number) requires a legal basis for each application. This leads to operational challenges in data processing, especially in the case of cross-organizational or cross-sectoral data processing. The introduction of a unique personal identifier has been hitherto prevented by privacy concerns. The debate has until now ignored the great dangers related to identification and data processing in state agencies. The multiplicity of special regulations allowing the use of the AHVN13 at federal, as well as at cantonal level, hinders to overview how and for which purpose the number is actually used.

The Bern University of Applied Sciences has received a mandate by the Swiss Information Technology Union[18] to provide a report, illustrating the risks and the costs arising due to the absence of a unique identifier in e-government processes. The report should also discuss the experiences made by other countries in using such an identifier, especially for cross-organizational and cross-sectoral use. Special interest is given to particular provisions aimed at securing privacy. The latter shall be investigated in 2-3 short semi-structured interviews with experts.

Objectives of this interview:

- Get an idea of the net value of having a national unique personal identifier.
- Get insights on experiences made related to privacy issues ever since the introduction of the national unique personal identifier.
- Get knowledge on provisions installed or to be installed to secure privacy.

In Denmark, every resident person has a civil registration number. The number is registered in the Civil Registration System (the CPR). The CPR contains basic personal data (full name, address, date of birth, marital status, nationality, etc.) about anyone with a civil registration number. Registration is made by local authorities. Any person is entitled to protection of name and address, local directories protection, opt-out of statistical, scientific surveys and marketing approaches. Information from CPR can only be disclosed according to law (permission granted by law and compliant with the Processing of Personal Data Act). Public authorities address their inquiries for CPR-Data to local authorities. Private individuals or entities that can prove their legal interest can be granted access to CPR-data by the Ministry of Economic Affairs and the Interior. As a resident, their CPR-number is relevant to apply for a NemID, a common secure login on the Internet to engage with businesses or public authority online.

In this respect, Switzerland would like to learn from the experiences of Denmark on the net value of having a CPR-number.

Interview Questions

7. Is the situation in Denmark as described above accurate?
8. Which processes and infrastructures in e-government are simplified through the use of a unique identifier (economic value)? What are the main benefits for the collaboration between state levels?
9. What other values and benefits are generated through the CPR-number (societal, cultural value)?
10. What are the main privacy concerns with the use of a unique identifier (identity theft, profiling, other)? Have any of the concerns been proven true? If yes, what were the consequences?
11. What provisions have been installed to secure privacy (legal technical, organizational)?

18 Assembly of cantonal ICT representatives

12. Based on your country's experiences, what recommendations would you give in order to secure the successful transformation of a social security number into a personal identifier?

Note
If approved by the interviewee, the phone call will be recorded for documentation purpose. To be defined with interviewee at the beginning or end of the interview.

Follow Up
To be discussed directly after the interview.

Annexe 5: Interview Guide ES

Introduction

Switzerland has no unique personal identifier. The use of the most common identifier of AHVN13 (the Swiss social security number) requires a legal basis for each application. This leads to operational challenges in data processing, especially in the case of cross-organizational or cross-sectoral data processing. The introduction of a unique personal identifier has been hitherto prevented by privacy concerns. The debate has until now ignored the great dangers related to identification and data processing in state agencies. The multiplicity of special regulations allowing the use of the AHVN13 at federal, as well as at cantonal level, hinders to overview how and for which purpose the number is actually used.

The Bern University of Applied Sciences has received a mandate by the Swiss Information Technology Union[19] to provide a report, illustrating the risks and the costs arising due to the absence of a unique identifier in e-government processes. The report should also discuss the experiences made by other countries in using such an identifier, especially for cross-organizational and cross-sectoral use. Special interest is given to particular provisions aimed at securing privacy. The latter shall be investigated in 2-3 short semi-structured interviews with experts.

Objectives of this interview:

- Get an idea of the net value of having a national unique personal identifier.
- Get insights on experiences made related to privacy issues ever since the introduction of the national unique personal identifier.
- Get knowledge on provisions installed or to be installed to secure privacy.

In Spain, every citizen over 14 years has National ID Card (DNI) which contains a 8+1 Digit Personal identification number. The number is also referred to as National Fiscal Number (NIF). Minors and foreigners do also obtain a NIF, referred to as NIE. The first version of a national identification number has been introduced in 1944. The NIF/DNI in the current form has been created in 1990 and is widely used for identification purpose in transactions with private and public entities. A sector specific identification number has been created for the health sector, but the DNI is often used instead of the health identification number.

In this respect, Switzerland would like to learn from the experiences of Spain on the use and benefits of the DNI/NIF.

Interview Questions

13. Is the situation in Spain as described above accurate?
14. Which processes and infrastructures in e-government are simplified through the use of a unique identifier (economic value)? What are the main benefits for the collaboration between the different state levels/different provinces?
15. What other values and benefits are generated through the DNI (societal, cultural value)?
16. What are the main privacy concerns with the use of the DNI (identity theft, profiling, other)? Have any of the concerns been proven true? If yes, what were the consequences?
17. What provisions have been installed to secure privacy (legal technical, organizational)?
18. Based on your country's experiences, what recommendations would you give in order to secure the successful transformation of a social security number into a personal identifier?

19 Assembly of cantonal ICT representatives

Note
If approved by the interviewee, the phone call will be recorded for documentation purpose. To be defined with interviewee at the beginning or end of the interview.

Follow Up
To be discussed directly after the interview.

Contrôle de version

Version	Date	Description	Auteurs
1.0	10.08.2015	Version définitive ; avant-projet pour consultation dans le groupe de travail de la CSI « Numéro AVS comme identificateur »	Angelina Dungga Thomas Selzam Olivier Brian Katinka Weissenfeld Jérôme Brügger Andreas Spichiger
2.0	30.09.2015	Version définitive	Angelina Dungga