Prof. Dr. David Basin: Évaluation des risques de l'utilisation du numéro AVS

Résumé

L'organisation et le traitement des données personnelles dans différents registres administratifs en Suisse ont évolué d'une manière problématique du point de vue de la protection des données. Des données personnelles, souvent sensibles, sont conservées dans plus de 14 000 registres tenus par des services administratifs ou d'autres organismes et indexés au moyen d'un identifiant unique, le numéro AVS à 13 chiffres (NAVS13). Les données et les systèmes informatiques utilisés pour les conserver peuvent faire l'objet d'attaques tant internes qu'externes ayant pour conséquence que des personnes non autorisées accèdent aux registres concernés. Ce risque est non négligeable, étant donné qu'un grand nombre des systèmes de conservation et de traitement des données contenues dans ces registres sont gérés par des organismes, tels que des administrations communales, des écoles et des hôpitaux, qui ne sont pas soumis à des exigences en matière de sécurité informatique aussi élevées que celles qui s'appliquent aux systèmes de la Confédération.

Le NAVS13 et les attributs relatifs à l'identité, tels que le nom, le prénom et la date de naissance, sont utilisés dans ces registres afin d'associer les individus à des données. En accédant à ces dernières, on peut donc savoir à quelles personnes elles se rapportent. Par ailleurs, l'utilisation du NAVS13 en tant qu'identifiant standard (là où son utilisation systématique a été autorisée) permet de relier facilement les données conservées dans différents registres et donne ainsi aux attaquants les moyens d'établir un profil détaillé des personnes concernées. Ces risques pour la protection des données vont se renforcer au fur et à mesure de l'augmentation du nombre d'organismes ayant recours au NAVS13 pour le traitement de données et de l'accroissement du volume de données collectées, conservées et traitées, en particulier par des administrations cantonales et communales et des organismes privés utilisant des systèmes informatiques non fédéraux relativement peu sûrs.

Les données des registres étant conservées avec les attributs relatifs à l'identité qui leur sont associés, le seul remplacement du NAVS13 par des identifiants sectoriels ou d'autres pseudonymes ne réduirait guère les risques pour la protection des données. Grâce à ces attributs, elles pourraient en effet toujours être rattachées de manière relativement précise aux personnes concernées. Il existe cependant des moyens de réduire considérablement ces risques. Ces moyens impliquent de repenser la manière dont les données sont conservées, traitées et sécurisées.

Les mesures suivantes permettraient de réduire nettement les risques qui pèsent aujourd'hui sur la protection des données, en particulier les risques consécutifs à l'expansion continue du mode actuel d'utilisation du NAVS13.

- L'une de ces mesures consiste à introduire des pseudonymes non signifiants (tels que le numéro de contribuable ou le numéro du dossier

électronique du patient) en respectant certains principes et à éviter autant que possible de les conserver dans les registres avec d'autres attributs relatifs à l'identité. Cette mesure peut être mise en œuvre en utilisant des identifiants sectoriels, qui peuvent prendre différentes formes.

- Certains processus administratifs et processus d'affaires nécessitent que les pseudonymes soient rattachés aux individus. La manière dont ce lien est établi et les conditions dans lesquelles il est établi doivent être soigneusement réglementées, tant au niveau technique qu'au niveau organisationnel.

- Une autre mesure consiste à fixer pour *tous* les systèmes traitant des données sensibles indexées au moyen du NAVS13 ou d'identifiants sectoriels des exigences en matière de sécurité et de processus d'assurance sécurité qui soient plus élevées que celles qui ont été définies par le Département fédéral de l'intérieur.

Ces mesures ont un coût. En particulier, les identifiants sectoriels ne sont pas aussi commodes et simples à utiliser que le NAVS13. Par ailleurs, l'utilisation d'identifiants sectoriels dans différents contextes implique une augmentation des coûts d'analyse, de conception et de mise en œuvre des systèmes, opérations nécessaires pour rendre compte de la manière dont les attributs relatifs à l'identité et les données personnelles sont utilisés dans les processus administratifs et les processus d'affaires et pour définir des procédures d'identification appropriées. Elle a également un impact sur la manière dont les organismes emploient leurs systèmes informatiques et la façon dont ils interagissent avec leurs clients. Pour pouvoir décider où et comment appliquer ces mesures, il faudrait procéder à une analyse coûts-bénéfices pour chaque scénario envisagé, ce qui sort du cadre de la présente étude.

En Suisse, la Confédération applique déjà l'ensemble de ces mesures dans différents secteurs dans lesquels des données personnelles sensibles permettant d'identifier les individus concernés sont traitées, ou mène des projets dans ce domaine. On peut mentionner comme exemples la pseudonymisation des données dans le cadre des analyses statistiques effectuées par l'Office fédéral de la statistique et les projets en cours portant sur l'introduction d'identifiants sectoriels pour les dossiers électroniques des patients et pour le registre du commerce. L'extension de ces mesures à d'autres secteurs est souhaitable dans une perspective de réduction des risques.

27 septembre 2017