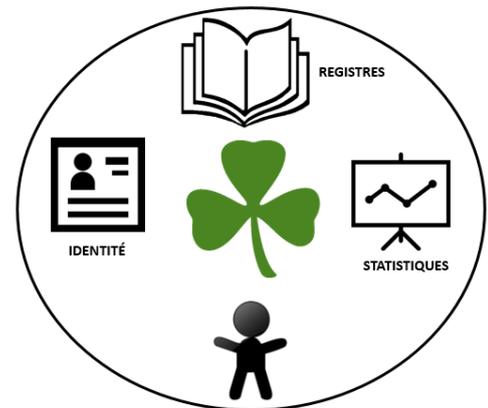


Leçon de chose sur l'Etat Civil IV : La protection des données personnelles

C'est fait ! Le mouvement ID4D (Identity for development) lancé conjointement par l'OMS et la Banque Mondiale vous a « emporté ». Désormais au fronton de votre administration en charge du projet de modernisation de vos registres d'état civil et de mise en place d'un registre de population, vient s'inscrire en lettre d'or : **garantir à tous d'ici 2030, une identité juridique, notamment grâce à l'enregistrement des naissances**, un des 17 objectifs de développement durable approuvé par l'ONU en Assemblée Générale.

Ce grand chantier que vous êtes en train de mettre en place auquel vous avez attaché le label onusien CR&VS pour *Civil Registry and Vital Statistics* a **un triple objectif** :

- Une identité pour tous et une infrastructure d'Etat Civil sécurisée et utilisée.
- La fourniture de statistiques vitales permettant aux autorités publiques d'orienter au mieux leurs actions, afin d'améliorer le sort « vital » des populations.
- L'élaboration d'un registre de population qui permette d'améliorer la productivité administrative, de faciliter la relation Administré-Administration ; un numéro unique d'identification d'Administré Citoyen complète le dispositif.



Il n'est pas de doute que cet investissement s'il est mené à son terme est gage d'efficacité et de meilleure gouvernance. L'objet de cette note n'est pas tant de tempérer votre volonté d'aller de l'avant, que de vous alerter sur l'existence d'un obstacle majeur que votre Administration va devoir « contourner » : celui de **la protection des données personnelles**.

1871201112



Le recours à un numéro unique d'identification est loin d'être universel et introduit un débat sur la recherche d'un équilibre entre des objectifs d'efficacité administrative et les menaces latentes contre les données de la vie privée.

Dans le monde, autant de pays, autant de cas d'espèce ; les pays ayant opté pour un registre de population centralisé se dotent généralement de ce code d'identification unique. Mais leur utilisation est le plus souvent strictement encadrée. De nombreux pays, mettent en œuvre des identifiants distincts par registre (social, fiscal, identitaire).

Le cas de la Suède prouve que l'on peut d'une part déployer de façon extensive la logique bureaucratique d'un numéro d'identification unique et d'autre part être un des pays précurseurs dans la protection des libertés individuelles.

Cas Suédois : *Un numéro d'identification personnel est attribué à toutes les personnes inscrites au registre d'état civil suédois. Les numéros d'identification personnels servent à l'identification dans la plupart des domaines, qu'ils soient publics ou privés. Les numéros d'identification personnels sont invariables et uniques, ce qui signifie que le numéro accompagne une personne tout au long de sa vie et qu'il n'existe pas deux numéros d'identification personnels identiques. Si une personne quitte la Suède et est désinscrite du registre d'état civil suédois, elle conserve son propre numéro d'identification personnel. Le numéro d'identification personnel doit figurer sur les déclarations fiscales, les déclarations de revenus et les autres documents soumis à l'administration fiscale suédoise.*

Le cadre juridique international de la protection des données personnelles a été fixé par l'ONU.

L'article 17 du Pacte international de l'ONU relatif aux droits civils et politiques (abrégé : Pacte ONU II)¹ ne protège que la vie privée, sans mentionner la protection des données².



Toutefois, l'Assemblée générale de l'ONU a adopté une résolution le 14 décembre 1990 qui fixe certains principes généraux en matière de fichiers personnels informatisés³.

Les deux éléments clefs de ce texte sont :

- Transparence vis à vis de l'utilisateur ; ce dernier doit avoir donné son accord de façon explicite à l'usage qui est fait de ses données personnelles
- La constitution d'un fichier doit répondre à une finalité, clairement présentée et justifiée à l'administré

C'est en général ce respect de la Finalité, qui est détaillé/complété dans les pays plus avancés en matière de protection des libertés individuelles, on y rajoute les principes de proportionnalité et de pertinence, tout en limitant dans le temps la durée de conservation des données.

Encore une fois, l'exemple suédois démontre qu'il est possible de conjuguer ces principes avec un usage intensif d'un numéro personnel d'identification dans tous les secteurs de la vie courante (banques, employeurs...)

Lors de la mise en place d'un projet de CR&VS, la protection des données personnelles n'est pas une priorité. L'architecte d'un projet CR&VS doit néanmoins anticiper l'évolution des mentalités et se préparer à un renforcement des protections des données individuelles, tâche d'autant plus mal aisée qu'elle se fait en méconnaissance des dispositions qui seront prises in fine.

Quatre principes peuvent d'ores et déjà être préservés :

1. Principe de Consentement

Les informations alphanumériques et biométriques qui sont collectées doivent l'être avec le consentement explicite de l'administré, qui doit être averti de l'usage qui est fait de ses données.

2. Principe de Traçabilité

La consultation des données personnelles doit pouvoir être tracée. Un fichier informatique sécurisé doit garder trace de toutes les consultations des données personnelles, même si elles ont pu être autorisées par voie judiciaire

¹ Pacte international relatif aux droits civils et politiques Conclu à New York le 16 décembre 1966 Approuvé par l'Assemblée fédérale le 13 décembre 1991 Instrument d'adhésion déposé par la Suisse le 18 juin 1992 Entré en vigueur pour la Suisse le 18 septembre 1992

² Art. 17 1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. 2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

³ Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, Adoptée le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990 ; <https://www1.umn.edu/humanrts/instreet/french/Fq2grcpd.html>

1

2

Follow us



3

3. Principe de Sécurisation

Les données personnelles doivent être archivées de façon sécurisée de telle manière qu'il ne soit pas possible de les altérer. L'idéal est que l'archivage soit dans le respect des réglementations existantes en matière d'archivage à valeur légale, en faisant donc appel aux technologies de signature électronique.

4

4. Principe d'Accès

Toute personne justifiant de son identité a le droit de savoir si des données la concernant font l'objet d'un traitement, d'en avoir communication sous une forme intelligible, sans délais ou frais excessifs, d'obtenir les rectifications ou destructions adéquates en cas d'enregistrements. Il faut donc aménager une procédure à cet effet.

