L'Identité Relationnelle

Que vaut notre système d'identification des personnes? En vérité pas grand-chose, parce que les papiers sont souvent faux et les contrôles peu ou pas efficaces. Les conséquences de la faiblesse de ce système sont désastreuses, en coût pour la collectivité mais aussi en termes de sécurité publique.

Il est si facile de se procurer des faux papiers qu'en France, pays pourtant champion de la lutte contre la fraude documentaire, la majorité des plus de deux millions de faux permis de conduire comptabilisés est aussi utilisée comme fausse pièce d'identité, et que la Police de l'Air et des Frontières intercepte à elle seule plus de dix mille faux documents par an en France.

Les faux papiers se répartissent en quatre grandes familles :

- ✓ la falsification (le fraudeur utilise un document authentique et change un élément, par exemple la photo ou état civil), qui est aujourd'hui la fraude la plus courante,
- ✓ la contrefaçon (reproduction à l'identique),
- ✓ le volé vierge (vol de documents entre l'imprimerie et l'administration)
- ✓ et l'usurpation d'identité (utilisation d'un document authentique perdu ou volé, ou délivré sur la base de faux justificatifs).

De nombreux documents sont même si faciles à reproduire qu'un simple scanner suffit à fabriquer la plupart de ceux qui permettent de se faire délivrer des documents d'identité authentiques. Les trafiquants proposent d'ailleurs des kits complets aux sans papiers, avec permis de conduire, carte Vitale et carte de résident.

Les documents d'identité biométriques ne sont qu'une toute petite partie de la solution puisqu'ils peuvent être délivrés sans correspondre à l'identité réelle des porteurs, avec de faux justificatifs.

Le contrôle d'identité en lui-même est une opération qui ne peut rassurer personne, comme le prouvent quelques exemples incontestables.

- ✓ A l'entrée d'un tribunal, des gardes dispensent de passer par les portiques de sécurité toute personne ayant une robe noire sous le bras et brandissant une carte d'avocat, de si loin qu'ils ne peuvent même pas faire la différence entre un vrai document et une mauvaise copie.
- ✓ Les réceptionnistes des immeubles de bureaux des entreprises ou des administrations nationales visant un document ne savent pas du tout comment différencier un vrai d'un faux, même lorsqu'il s'agit d'un document français comme une carte nationale d'identité.
- ✓ Même les services de sécurité d'un ministère sensible ne peuvent pas faire grand-chose lorsqu'on leur présente un document authentique mais qu'il n'existe qu'une ressemblance entre le porteur du document et son titulaire.

Le coût pour la collectivité est considérable, parce que la fraude documentaire permet tous les abus, de l'obtention de prêts sur la base de fausses fiches de paie à l'usurpation d'identité, en passant par la conduite sans permis ou sans assurance, le vol de voitures, la perception de prestations sociales indues, l'entrée au domicile de personnes fragiles, et est un moyen indispensable pour nombreuses formes de banditisme, de violence et de terrorisme.

Il est donc temps de changer de méthode. La solution proposée ici est l'identité dite « relationnelle » parce qu'elle est fondée sur les témoignages de personnes qui connaissent le titulaire du document et peuvent garantir son identité.

A l'heure d'Internet, c'est possible, et je vais m'attacher à expliquer comment cette solution qui diminuerait considérablement le coût de la fraude pour la collectivité et surtout les risques liés au grand banditisme et au terrorisme, peut respecter les libertés fondamentales, mieux encore que les organisations régaliennes.

A l'heure d'Internet, il est facile de conserver un grand nombre de données dans des serveurs sécurisés disposés à travers le monde, et d'empêcher tout croisement de fichiers qui ne respecterait pas le principe du respect des informations personnelles.

Le concept d'Identité relationnelle repose sur les quatre règles suivantes.

1. L'identité basée sur des témoignages

   L'identité d'une personne est garantie par de nombreux tiers : des états, des collectivités, des entreprises, mais aussi et surtout des amis et membres de la famille.

   Ces tiers peuvent aussi délivrer un témoignage d'honorabilité, consistant à certifier qu'à leur connaissance, la personne considérée n'a pas d'activité maffieuse ou terroriste.

2. La notation de la qualité de chaque identité

   Une identité bénéficie d'une notation qui est fonction du nombre et de la qualité des témoignages recueillis, selon un barème mis au point par un jury indépendant composé de personnalités qualifiées. Ce barème pourra évoluer au fil des années.

3. Le choix par chacun du ou des tiers de confiance conservant leurs éléments d'identité

   Les éléments d'identité d'une personne sont stockés sur le cloud, chez des tiers de confiance choisis par le titulaire et pour certains éléments par les autorités régaliennes (l'état civil par exemple).

   Le principe selon lequel les éléments d'une base de données ne peuvent être transférés dans une autre base de données étant respecté, les éléments d'identité peuvent être riches et nombreux : état civil, adresses, liens Internet, numéros de téléphone, mais aussi diplômes, certificats, relevés bancaires, dossier médical, etc..

   Un titulaire peut conserver chez des tiers de confiance différents ses informations personnelles, selon leur nature. Voici quelques exemples :

   - ✓ informations d'état civil, adresses internet, numéros de téléphone, etc.
   - ✓ dossier de santé,

- ✓ contrats de travail, fiches de paie et certificats de travail
- ✓ diplômes
- ✓ informations financières et bancaires,
- ✓ liste de biens assurés,
- ✓ etc.

Sur demande du titulaire, ces tiers de confiance spécialisés peuvent vérifier les informations communiquées, et en attester la valeur. C'est par exemple le cas de celui choisi pour conserver les informations d'état civil, qui peut vérifier l'authenticité des documents d'identité fournis.

Le titulaire peut aussi choisir un partenaire appelé « Registrar » qui est chargé d'établir la relation entre son identifiant principal (un pseudo ou des éléments d'état civil) et les tiers de confiance choisis par lui. C'est le Registrar qui fournit les cartes comportant la clé permettant au titulaire d'accéder au système.

4. La maitrise par le titulaire de la communication d'éléments de son identité

   Les individus disposent d'une ou plusieurs clés leur permettant d'accéder à leurs éléments d'identité et d'en ouvrir des accès ponctuels ou durables à des tiers, afin de prouver leur identité et/ou leurs qualités. Ce sont eux qui autorisent ou non un transfert d'un élément d'identité par l'un ou l'autre de leurs tiers de confiance à un tiers.

Comment ça marche

Dans la pratique, lorsqu'une personne souhaite prouver son identité ou une qualité, elle présente sa carte à un tiers qui la lit avec un simple smartphone, avec une application universelle gratuite d'identification qui permet de vérifier qu'il s'agit bien de l'original de la carte.

Ce tiers peut alors voir sur l'écran la photo du titulaire et la notation de son identité, et indiquer des éléments d'identité dont il souhaite obtenir communication.

Avec la même application, qui est protégée par un code PIN, le titulaire voit ces demandes de communication et donne ou non son accord.

En cas de perte ou vol de sa carte, le titulaire peut l'annuler sans délai par Internet. Il a alors besoin de l'assistance de plusieurs de ses relations – désignées par avance par lui - pour en mettre une autre en service. Ces relations seront questionnées par Internet pour vérifier que le titulaire les a bien prévenus de son choix de changer de carte.

Le titulaire peut disposer de plusieurs cartes correspondant à différentes collections d'informations d'identité. Une carte choisie par lui pour communiquer ses informations médicales étant par exemple essentielle pour pouvoir lui demander des informations médicales détaillées.

Une application concerne les cartes professionnelles : une carte du titulaire peut donner automatiquement accès à l'affichage de sa photo et confirmer sa fonction : c'est par exemple un policier ou un pompier, ou une infirmière diplômée.

Les faux papiers deviennent impossibles à fabriquer, puisqu'il n'y a tout simplement plus de document d'identité. La carte n'est qu'une clé donnant accès aux éléments d'identité lesquels sont stockés sur des serveurs sécurisés.

La sécurité du système repose sur l'intégrité des serveurs, mais aussi et surtout sur la certification des informations.

- L'intégrité des serveurs sur lesquels sont stockées les informations d'identité.

  Certains sont gérés par des états, d'autres par des opérateurs privés choisis par le titulaire.

- La certification des informations

  Chaque information peut ou doit, selon sa nature, être assortie d'une certification. Un diplôme ou un certificat doit par exemple certifié par son émetteur ou par une autorité de certification indépendante.

Toutes les technologies existent pour mettre en service cette nouvelle organisation sans tarder :

- le cloud et ses moyens de sécurisation,
- les cartes impossibles à recopier et authentifiables par smartphone,
- les smartphones et les applications permettant l'authentification des cartes, dont en particulier la prochaine version de l'application IPM de l'Organisation Mondiale des Douanes.

Les entités nécessaires à l'accomplissement des principales fonctions existent :

- les fournisseurs de services numériques susceptibles de jouer le rôle de "Registrars", conservant la liste des tiers de confiance retenus par chaque titulaire et pouvant assurer le lien après authentification d'une carte,
- les tiers de confiance,
- les sociétés de certification,
- et surtout les individus souhaitant bénéficier d'une carte d'identification numérique gratuite.

Le financement de l'opération est largement assuré par une contribution versée aux fournisseurs de services numériques en assurant le fonctionnement, par les tiers de confiance, par les sociétés de certification et par tous les tiers souhaitant bénéficier des nouvelles possibilités de vérification d'identité et d'acquisition auprès des titulaires des informations nécessaires à leur activité.

Enfin, l'aspect relationnel de l'organisation, qui donne toute leur valeur aux identités, comporte aussi un moyen pour la police de remonter des filières maffieuses et terroristes.

9 décembre 2015