L'union controversée de l'identité et de la biométrie

- Technologie -

Date de mise en ligne : vendredi 7 juillet 2006

Fiabilisée grâce aux empreintes digitales, la carte d'identité électronique, soulève des questions de société et s'accompagne d'incertitudes techniques.

Face à la fraude documentaire et au vol d'identité, dans un contexte de menace terroriste, le projet de carte nationale d'identité électronique (CNIE) refait surface. Elaboré par le ministère de l'Intérieur, il entend fiabiliser la carte d'identité en recourant à la biométrie, avec un archivage national. Le remède se révélera-t-il pire que le mal ?

La biométrie n'est pas une technologie comme les autres. Elle rend plus difficile la préservation de l'anonymat et de la vie privée, sans compter que, reposant sur des probabilités, elle est susceptible d'erreurs. La solution est en cours de discussion. Elle sera soumise à la Commission nationale de l'informatique et des libertés (Cnil) et au législateur.

La CNIE serait facultative. Elle enregistrerait les empreintes des deux index et la photo du visage. Des informations biométriques (empreintes de six doigts, et photo) seraient également conservées dans une base, afin de vérifier qu'une personne qui renouvelle sa carte le fait avec la même identité que précédemment. L'accès à cette base serait étroitement encadré, juridiquement et techniquement, afin de protéger les libertés individuelles.

Les employés de mairie, notamment, n'y accéderaient pas. On respecterait alors le cadre réglementaire français : pas de fichier exhaustif de tous les citoyens, pas d'identifiant unique d'une personne auprès des administrations, pas d'interconnexion des fichiers et pas de carte d'identité obligatoire. La solution pourrait aussi fonctionner sans une base centrale biométrique, mais avec une fiabilité moindre.

Un certificat électronique optionnel

En outre, la CNIE donnerait à son possesseur un accès à des droits ou à des données personnelles sur internet (dossier médical ou fiscal, compte bancaire), grâce à un certificat électronique optionnel. La signature électronique, quant à elle, nécessite des approfondissements. Le ministère espère lancer la CNIE fin 2008, afin d'optimiser les coûts en s'alignant sur le calendrier européen de passeport électronique intégrant les empreintes en 2009.

Mais, si l'Europe prévoit l'usage des empreintes digitales, leur acceptation ne va pas de soi. En Belgique, où 2,5 millions de cartes d'identité électroniques sont en activité, les empreintes ont été écartées, afin d'éviter un sentiment de fichage. Un paradoxe puisque nos voisins sont tous identifiés dans un registre national (RN).

En mai, une audition menée par l'office parlementaire français d'évaluation des choix technologiques a permis aux différentes opinions de s'exprimer. Elles vont de la défiance face à la biométrie jusqu'à l'affirmation de son inéluctabilité, sans oublier les intérêts de nos champions industriels nationaux.

Pour Alain Weber, représentant de la Ligue des droits de l'homme, « les dérives sont inhérentes à la biométrie ». Il en veut pour preuve l'expérimentation Biodev. Soixante mille demandeurs de visas ont reçu un titre électronique intégrant les empreintes de leurs dix doigts et leur photo. Puis, deux mille cinq cents officiers de police ont eu accès à cette base des visas. « D'une prévention de la fraude documentaire, on aboutit à un fichier de police », déplore-t-il.

Quant à la Cnil, elle interroge : quelle est la finalité de la CNIE ? « S'agit-il de délivrer un titre fiable, ou de posséder un fichier d'identification policière ?, s'enquiert Christophe Pallez, son secrétaire général. Dans le premier cas, le

raisonnement du ministère de l'Intérieur, qui l'amène à constituer une base d'empreintes, n'est pas encore convaincant. »

Il admet cependant qu' « une base centrale est nécessaire » pour s'assurer de l'unicité d'un titre, à condition qu'elle s'accompagne d'anonymisation ou d'accès unidirectionnel. « Sans exclure des conditions d'accès restreint de la police ou de la justice, au cas par cas, ce qui nécessite de détailler des procédures. »

L'anonymisation interdira de remonter à une personne à partir d'empreintes, et inversement, sans sa CNIE. On évitera ainsi d'être convoqué au commissariat pour avoir laissé ses empreintes au mauvais endroit au mauvais moment. Une solution consiste à séparer la base biométrique de celle des identités, en interdisant un lien direct entre elles. Ce principe séduit le ministère. Un industriel, Sagem, propose un procédé ad hoc.

Baptisé « lien faible », il confirmera avec une très forte probabilité qu'une personne revendique une identité à juste titre, par exemple lors du renouvellement d'une CNIE perdue ou abîmée. Quant à l'accès unidirectionnel, il retrouve les empreintes d'une personne à partir de son identité grâce à un pointeur vers la base biométrique.

Les limites pratiques

Sur le papier, cela fonctionne. Mais des obstacles subsistent. D'abord, la biométrie ne supprime pas les risques d'usurpation ou même d'invention d'identité lors de la première demande d'une CNIE. « Rien de plus facile que d'employer de faux justificatifs sur papier », reconnaît-on au ministère. Cette phase devra donc être durcie.

Autre bémol, les performances et l'interopérabilité des systèmes de vérification des empreintes digitales doivent s'améliorer. Quant aux politiques, ils tiennent des propos contradictoires. Certains voient dans le système un moyen d'identifier les victimes de catastrophes, sous contrôle d'un magistrat. Or, un « lien faible », protecteur des libertés publiques, empêche de retrouver une personne par ses empreintes.

Enfin, les autres garde-fous envisagés ont leurs limites. Première idée : la CNIE est facultative, et les titres papier demeurent. Cela ne convainc pas Alain Weber : « Le système papier disparaîtra au profit de la biométrie, si des facilités lui sont associées. » Seconde idée : les citoyens pourront vérifier qui a consulté leur dossier, et les abus seront sanctionnés. La Belgique a mis en place une solution de ce type pour son RN.

La sécurité sociale ou les syndicats y ont accès, mais pas les banques ni les huissiers. Quant aux consultations des dossiers par la sécurité du territoire et la police, le citoyen n'en sera pas averti. Denis Van Melsen, chef de projet de la carte d'identité électronique belge, a été victime d'une mésaventure révélatrice. « Les responsables d'une collectivité locale que je devais rencontrer ont consulté mon dossier. Cela est inadéquat, et je leur en ai fait part. Mais, désormais, une déontologie se met en place dans l'accès au RN. » Un apprentissage qui n'a rien de rassurant.

Le passeport européen associe photo et empreintes

À l'heure où la France discute sur l'intégration des empreintes dans la CNIE, c'est la photo du visage qui a été retenue afin de fiabiliser les passeports au niveau international.

Une puce sans contact placée dans le document mémorisera cette photo. Le douanier vérifiera la concordance entre la personne, la photo imprimée et celle qui est enregistrée. La puce ne sera lisible qu'une fois le passeport ouvert.

Elle sera déverrouillée grâce à une clé secrète lue sur le document. Une autre modalité biométrique est acceptée.

L'Europe a opté pour les empreintes (des 2 index). Le passeport arrive en tête des pièces administratives (permis de conduire, carte de santé, carte d'identité, visa, etc.) qui adoptent une puce électronique. Le secteur de la sécurité et de l'identité devrait progresser de 30 à 50 % cette année. Le marché gouvernemental est le plus important, comparé à celui des entreprises.

Une connaissance statistique de l'être humain

De nouveaux indicateurs biométriques ne cessent d'apparaître. Les empreintes digitales sont souvent citées comme les plus performantes. Mais les spécialistes travaillent aussi sur l'iris, le visage (en 2D ou 3D), la forme de la main, la géométrie de l'oreille, les veines des bras, la voix... Ces indicateurs nécessitent une connaissance statistique du corps humain, car on doit s'assurer que la probabilité d'une même signature biométrique pour deux personnes soit infime sur des populations de plus de quarante millions d'individus.

Selon le nombre de points de comparaison retenus, en matière d'empreintes digitales, cela entraîne la prise en compte de plusieurs doigts, deux étant insuffisants. Il faut également noter que de 2 à 3 % d'une population est inadaptée à un type de biométrie. Dans le cas des empreintes, il peut s'agir de personnes ayant eu les doigts coupés ou brûlés par des acides...

Cela justifie également le recours à la multimodalité. Plus coûteuse, elle associe plusieurs indicateurs biométriques afin de réduire les risques d'erreurs.

Post-scriptum :

http://www.01net.com/article/321830.html