

# Droit des technologies avancées

## Protection de l'identité v. Dignité numérique

Par [Alain Bensoussan](#) le 13 janvier 2012 13h32 | [2 Commentaires](#)

Constituer un fichier biométrique de la population pour mieux garantir l'identité est, à l'heure du numérique, un véritable défi pour une démocratie.

### La légitimité d'un fichier biométrique

L'état actuel des fraudes documentaires justifie que l'on s'intéresse à la protection de l'identité numérique. Elle s'impose même face à l'ampleur du phénomène. En France, on estime à 200 000, le nombre annuel de victimes de fraudes à l'identité.

La proposition de loi vise à créer une future carte nationale d'identité qui sera dotée de deux puces. L'une obligatoire, régaliennne, contenant l'état civil du porteur mais également sa photo et ses empreintes digitales numérisées. L'autre, optionnelle, qui sera dédiée à l'e-commerce et permettra au porteur d'effectuer des transactions en ligne via un lecteur de cartes spécialement adapté.

Pour fonctionner et assurer l'authentification des données, il faut créer une base centrale des « Titres électroniques sécurisés » (TES), dont le rôle sera de « recenser, confronter, vérifier les informations » afin de détecter les usurpations d'identité ou les falsifications de documents.

La base TES est destinée à recenser, de manière unique et centralisée, les éléments d'état civil et les données biométriques fournis par chaque demandeur ou titulaire d'un titre d'identité.

La [proposition de loi](#) qui a été adoptée par l'Assemblée nationale le 12 janvier 2012, a rétabli la possibilité de faire correspondre données biométriques et données biographiques, possibilité de croisement que les sénateurs avaient supprimée.

Le bras de fer entre l'Assemblée nationale et le Sénat risque de se prolonger, le texte devant maintenant repartir au Sénat, qui va vraisemblablement s'en tenir à sa position. Si tel est le cas, la proposition de loi devra alors être de nouveau examinée par chacune des deux assemblées, avant d'être définitivement adoptée par les députés.

### Le principe de proportionnalité face à la nécessité

La base nationale TES illustre le problème de la proportion entre sécurisation de l'identité et risque d'atteinte aux libertés. Il faut trouver les moyens de protéger l'identité des personnes sans porter atteinte à leurs libertés fondamentales.

Le principe de légitimité ne doit pas dominer le principe de proportionnalité. Pour le Conseil d'Etat, dans sa [décision](#) du 26 octobre 2011, sous réserve du respect du principe de proportionnalité, la base TES a une finalité de sécurité tout à fait légitime.

Certes, le Conseil d'Etat a estimé que le système centralisé TES était en adéquation avec les finalités légitimes du traitement et que, s'il portait une atteinte à la vie privée, celle-ci n'était pas disproportionnée par rapport à l'objectif poursuivi, à savoir la protection de l'ordre public.

Il a néanmoins ordonné la destruction des empreintes prélevées en surnombre, considérant, au titre de la proportionnalité, que deux empreintes suffisent à établir un document d'identité.

Dans une démocratie numérique, la lutte contre l'usurpation et la falsification d'identité a ses limites. Il y a nécessairement une frontière à ne pas dépasser, même pour des besoins légitimes de protection. On est en droit de s'interroger sur le fait de savoir si le fichage potentiel de 45 millions « d'honnêtes gens », pour

reprendre la formule entendue lors des débats, n'est pas disproportionnée.

On sait que la vitesse de développement des fichiers est inversement proportionnelle au développement du cadre juridique de leur régulation.

Le dernier [rapport d'information](#) parlementaire, déposé à l'Assemblée nationale le 21 décembre 2011, sur les fichiers de police montre que le nombre de personnes fichées est en constante augmentation. La France compte actuellement 80 fichiers de police, dont 45% n'ont pas encore de base légale.

La nouvelle base TES pourrait se transformer en outil dangereux et liberticide du fait des interconnexions avec d'autres fichiers. Elle doit donc être encadrée de façon à trouver un juste équilibre entre la protection des libertés et la sécurité dans le domaine de l'usurpation d'identité.

Il pourrait y avoir disproportion si la base TES dépassait le rôle imparti de fichier « administratif » servant à délivrer des cartes d'identité pour devenir un fichier de police. Or, la limite n'est-elle pas en passe d'être atteinte si l'on permet l'utilisation judiciaire de la base TES pour les enquêtes de police relatives aux usurpations ?

C'est l'un des points de dissension entre le Sénat et l'Assemblée nationale que la Commission mixte paritaire n'est pas encore parvenue à arbitrer.

### **Les garde-fous envisagés**

En l'état du projet, il semble que le Gouvernement ait décidé de retenir, pour la carte d'identité électronique, la même limitation fixée par le Conseil d'Etat, soit deux empreintes prélevées et enregistrées, pour garantir une proportionnalité entre les objectifs et les moyens.

Par ailleurs, la reconnaissance faciale semble également totalement exclue du traitement, ainsi que la Cnil le préconisait. Ainsi, le traitement ne comporterait pas de dispositif de reconnaissance faciale à partir des images numérisées du visage qui sont enregistrées dans la base.

Enfin, la proposition de loi encadre les réquisitions judiciaires qui portent sur la base TES. Ainsi, les magistrats ne pourraient y avoir accès que pour des recherches en matière de fraude identitaire. La consultation du fichier ne serait pas élargie à toute réquisition judiciaire.

La base serait consultée sous le contrôle d'un magistrat, dans le cadre d'enquête de flagrance, d'enquête préliminaire ou sur commission rogatoire, liées à des infractions de fraude à l'identité (atteinte à la personnalité, atteinte aux services spécialisés de renseignement, atteinte à l'état civil des personnes, etc.).

### **Les garde-fous préconisés**

Il est clair que le législateur devra augmenter les garanties légales pour éviter toute dérive qui pourrait survenir en présence d'un Etat sous pression nationaliste. En l'état, les garde-fous envisagés ne semblent pas suffisants.

Pour renforcer les mécanismes de protection, quelques règles devraient être explicitement inscrites dans la loi :

- interdiction totale d'interconnexion avec le fichier de la sécurité sociale, baptisé Répertoire national commun de la protection sociale (RNCPS), sensé lutter contre les fraudes ;
- interdiction de croiser la base TES avec les autres fichiers ou recueils de données nominatives ;
- traçabilité de tous les accès à la base TES avec justification des accès par une authentification forte ;
- possibilité de recours des individus par un référé spécial ;
- renforcement de la régulation en donnant une compétence à la Cnil, qui fera des audits qu'elle rendra publics dans son rapport annuel.

Les restrictions d'accès des personnes habilitées dans le strict cadre de leurs fonctions et attributions légales, est un des éléments de garantie. Il conviendrait d'affecter deux magistrats désignés par des hautes juridictions administratives et judiciaires (Conseil d'Etat, Cour de cassation notamment).

La possibilité pour tout un chacun de former des recours serait également un élément de régulation d'une démocratie numérique, de même que l'instauration d'un contrôle populaire sous la forme d'une commission, dont les membres issus de tous les courants de pensée de la société française seraient désignés par des autorités administratives indépendantes, de hautes instances nationales et européennes - y compris du monde religieux - (Cnil, Commission nationale consultative des droits de l'homme, Assemblée nationale, Sénat, Conseil économique et social, Commission européenne, Conseil de l'Union européenne, Conférences des évêques de France, etc.).

Il faut en effet pouvoir rendre compte de l'exigence démocratique du respect de la dignité numérique.

**Tags:** [atteinte à la vie privée](#), [base TES](#), [dignité numérique](#), [falsification de document](#), [fichier administratif](#), [fichier biométrique](#), [fichier de police](#), [fraude identitaire](#), [identité numérique](#), [titre d'identité](#), [titre électronique sécurisé](#), [usurpation d'identité](#)

## Partager

## 2 commentaires

[COPIN](#) | [16 janvier 2012 9h20](#) | [Répondre](#)

Les auteurs souhaitent renforcer le contrôle en créant de nouvelles structures censés mieux protéger le citoyen. C'est le mal français que de rajouter de nouvelles structures à celles déjà existantes. De quoi reclasser des femmes et des hommes à la recherche de pouvoir ou de revenus supplémentaires.

L'attitude de l'opposition me semble claire : la mise en doute systématique des forces de sécurité et de la magistrature et l'aveuglement idéologique par des références à un passé douloureux.

### Rappel des faits

En rédigeant la proposition de loi sur la protection de l'identité, le Sénat souhaitait que cette protection soit efficace et réaliste. Pour juguler, voire empêcher la fraude à l'identité, l'idée est de faire en sorte que lors d'un contrôle l'autorité chargée de l'effectuer puisse consulter un fichier contenant les empreintes digitales des titulaires de cartes nationale d'identité. C'est ce qu'on appelle un fichier à "lien fort". Pour encadrer cette consultation, le Sénat puis l'Assemblée nationale a entouré cette possibilité de consultation d'obligations juridiques avec la mise en œuvre d'un système de traçabilité des consultations de ce fichier. Par ailleurs, comme le rappelle les auteurs de cet article " la base serait consultée sous le contrôle d'un magistrat, dans le cadre d'enquête de flagrance, d'enquête préliminaire ou sur commission rogatoire, liées à des infractions de fraude à l'identité (atteinte à la personnalité, atteinte aux services spécialisés de renseignement, atteinte à l'état civil des personnes, etc.) ".

Toutes les garanties ont été prévues pour protéger le citoyen.

Pour le Sénat, désormais dans l'opposition, ce n'est pas suffisant. Ce qui laisse à penser que l'opposition et quelques brebis égarées de la majorité n'accordent aucune confiance dans le respect du citoyen par les forces de sécurité et les magistrats.

Les sénateurs ont sauté sur l'occasion d'une idée, un concept jamais testé, et dont l'efficacité est contestée par celui qui l'a proposé : celui de la base de données à "lien faible". Dans ce cas, lors d'une consultation de la base, le système répond que cette empreinte contrôlée existe, sans préciser à quel citoyen elle correspond.

Ainsi, dans ce cas, en cas d'usurpation d'identité, on comprend qu'il y a un délit, donc une victime, mais on ne sait pas qui est l'auteur de ce délit, contrairement au lien fort. Pour simplifier, ces empreintes digitales sont rangés dans des classeurs où sont stockés plus d'une centaine d'empreintes. Dans le cadre du lien faible, les

enquêteurs devront analyser toutes les empreintes digitales du classeur pour remonter à l'usurpateur. Au delà des dépenses occasionnées par le travail de dizaines d'enquêteurs, tous les "gens honnêtes" du classeur seront interrogés.

Au delà de ces considérations, il semble que de nombreux parlementaires n'ont pas saisi l'enjeu posé par le thème de la protection de l'identité des citoyens aujourd'hui. Avec l'informatique, l'arrivée de l'Internet et leur corollaire, la dématérialisation de l'information, nous sommes entrés dans un monde nouveau. L'une des conséquences de cette situation est que le contrôle de l'identité du citoyen n'est plus l'apanage, la chasse gardée des forces de sécurité. Le contrôle d'identité est le plus souvent réalisé par les administrations et les entreprises publiques et privées. La présentation d'un document d'identité est exigée lors de toute transaction contractuelle entre ces organisations et le citoyen contractant. Qu'il s'agisse d'une demande de logement, du retrait d'un mandat ou d'un colis postal, de la souscription d'un crédit, de l'ouverture d'un compte bancaire et d'un abonnement téléphonique... Toutes ces organisations exigent la présentation d'un document attestant de notre identité. Mais ce qui est grave et générateur de production de faux titres, c'est la production de photocopies de ces titres qui vont traîner dans des dossiers administratifs sans aucune protection, à la portée du dernier stagiaire venu. On peut affirmer que nous avons tous plusieurs photocopies (10, 20 ou plus?) de nos documents d'identité rangés dans des dossiers laissés sans contrôle.

Ce qu'il manque à la protection de l'identité ce n'est pas de nouvelles structures chargées de contrôler ce qui l'est déjà, mais l'obligation faite à toute organisation impliquée dans une relation contractuelle de se doter de dispositif de lecture des documents d'identité présentés par le contractant. Ce qui éviterait la production de ces millions de photocopies dangereuses et éviterait la tentation d'usurpation d'identité.

Il faut se poser deux questions fondamentales : à quoi la puce de la carte bancaire aurait servie si les commerçants ne s'étaient équipés de dispositifs de contrôle de cette puce ?

Une dernière question : qui a contrôlé votre identité ces cinq dernières années, et pourquoi ? Les forces de sécurité ou les organismes et entreprises publiques et privées ?

---

[Quelle proportionnalité ? | 7 février 2012 11h14 | Répondre](#)

La CNIL a beau jeu de mettre en avant le principe de proportionnalité entre sécurisation de l'identité et risque d'atteinte aux libertés. Mais les technologies qu'elle admet ne respecte en rien cette proportionnalité. Un exemple flagrant est le fait d'encourager le système de reconnaissance des parties veineuses de la main dans les cantines des écoles. Peut-on parler de proportionnalité raisonnable dans un exemple comme celui-ci ? L'exercice de l'intimité identitaire est-il respecté ?

---