

Ligue des droits de l'homme (LDH),
Syndicat de la magistrature (SM),
Syndicat des avocats de France (SAF),
association *Imaginons un réseau internet solidaire* (IRIS),
intercollectif *Droits et libertés face à l'informatisation de la société* (DELIS)
Association française des juristes démocrates (AFJD)

INES

de la suspicion au traçage généralisé

Le 1^{er} février 2005, à la demande du ministère de l'Intérieur, un débat public a été ouvert sur Internet et par des réunions publiques en région, au sujet du projet de ce ministère baptisé « INES » (identité nationale électronique sécurisée), qui vise à créer une carte d'identité électronique à éléments biométriques.

Cette nouvelle carte d'identité serait équipée d'une puce électronique, lisible sans contact, et contiendrait des éléments d'identification biométriques personnels (empreintes digitales et photographie numérisée). Ces éléments numérisés seraient conservés dans un fichier central. Réunissant plusieurs fonctionnalités, cette carte constituerait un nouveau « Sésame ». Sont ainsi prévues non seulement une fonction d'identification sécuritaire, mais aussi des fonctions de signature électronique destinées à permettre, d'une part, l'accès à des prestations administratives par Internet et, d'autre part, l'authentification de transactions commerciales conclues par voie électronique. Enfin, la carte d'identité inclurait aussi un portefeuille électronique personnel permettant le stockage volontaire de données diverses.

Un débat de façade

Pour imparfait et cantonné aux initiés qu'il soit, un débat est en cours. Sans en attendre la synthèse, prévue pour le début du mois de juin, le Premier ministre a validé le projet au cours d'un comité interministériel le 11 avril dernier. Il a en outre annoncé la perspective de rendre cette nouvelle carte obligatoire. Comme souvent, le débat vise ainsi moins à soumettre un projet aux implications nombreuses et complexes à une discussion citoyenne réellement ouverte, qu'à orchestrer la légitimation d'une décision gouvernementale

déjà prise, non seulement dans son principe, mais encore pour l'essentiel de ses modalités. Quand les seules questions qui restent éventuellement en discussion sont celles du caractère obligatoire ou payant de ce nouvel outil, qui pourra croire que le débat est ouvert sur la nécessité de recourir à une carte à puce, lisible sans contact, de banaliser l'utilisation d'éléments biométriques personnels numérisés, non seulement pour des applications sécuritaires comme le contrôle d'identité, mais encore dans des applications à but purement commercial ?

Les alibis de la fraude et du terrorisme

Le caractère à bien des égards incantatoire, voire purement fallacieux, des arguments avancés pour justifier le recours à ces nouvelles technologies, vient conforter l'impression qui se dégage du caractère purement formel du débat initié.

Ce projet serait dicté par la préoccupation de lutter contre d'importantes fraudes ou falsifications de titres d'identité. Cependant, malgré l'importance qu'il attribue à ce phénomène, le ministère de l'Intérieur, de son propre aveu, ne paraît pas en état d'en évaluer précisément l'ampleur, qui reste à établir par des études objectives. Sans avoir démontré la réalité du problème, il propose de recourir à une solution coûteuse à la fois financièrement et en termes de libertés

publiques. Pourtant, la transmission directe des actes de naissance entre les services d'état civil et les services chargés d'établir la carte d'identité constituerait à la fois une simplification administrative pour l'usager et une garantie contre l'obtention frauduleuse d'une carte d'identité par la production d'un acte de naissance usurpé ou falsifié. En quoi une telle solution, moins problématique, serait-elle insuffisante ?

De la même manière, aucune donnée précise n'est avancée en ce qui concerne l'ampleur et la nature des fraudes à l'identité qui seraient cause de préjudices économiques importants résultant de l'obtention induite de prestations sociales diverses ou d'escroqueries dans des transactions commerciales.

La carte d'identité actuelle avait déjà été présentée comme « infalsifiable ». Le souvenir de cette promesse ne peut donc que nous incliner à la prudence sur ce sujet, surtout si l'on en croit le ministère de l'Intérieur. L'ampleur prise par les falsifications de cartes bancaires, la falsification des nouveaux billets en euros, eux aussi « infalsifiables », nous ont depuis longtemps démontré le caractère relatif de cette notion. Au contraire, la complexification des dispositifs de sécurisation rend la falsification plus difficilement détectable, avec le risque de préjudices beaucoup plus importants du fait de la confiance particulièrement forte accordés à ces nouveaux titres.

L'argument tiré de la lutte contre le terrorisme constitue aussi un pur alibi. Il est ainsi faux de prétendre que la nouvelle carte d'identité électronique serait imposée par la réglementation Européenne et les règles de l'organisation de l'aviation civile internationale qui ont conduit l'Union Européenne à instaurer des visas et des passeports incluant des éléments d'identification biométriques. Au contraire le règlement européen du 13 décembre 2004 réserve expressément la compétence des Etats membres en ce qui concerne les cartes d'identité. S'il est vrai que la carte d'identité peut servir de document de voyage alternatif au passeport pour certaines destinations, cela ne justifie pas d'appliquer les mêmes dispositions aux deux documents. Ce choix n'est d'ailleurs pas celui d'autres pays européens, dont les ressortissants peuvent également utiliser leur carte d'identité comme titre de voyage. Par ailleurs, la fraude à l'identité constitue un moyen parmi de nombreux autres qu'utilisent les réseaux terroristes, et certes pas le plus courant : doit-on rappeler que dans la quasi-totalité des attentats les plus violents, leurs auteurs ont utilisé leurs propres identités ? Rien ne démontre la prépondérance de cette fraude ni, par conséquent, en quoi la sécurisation à l'extrême des titres d'identité permettrait de lutter efficacement contre l'existence de réseaux criminels.

Les justifications avancées apparaissent donc particulièrement fragiles. Cette fragilité est révélatrice des logiques qui sous-tendent en réalité un tel projet.

Le contrôle d'identité banalisé

La carte d'identité électronique participera avant tout au renforcement et à la multiplication des contrôles d'identité. Aujourd'hui chacun peut faire la preuve de son identité par tous moyens. Le contrôle de l'identité, bien que largement banalisé dans les faits, reste juridiquement encadré et ne

peut être réalisé que dans des conditions précises. Enfin, si la carte actuelle offre une fonctionnalité de lecture optique, celle-ci n'a jamais été effectivement mise en œuvre. Son utilisation est normalement limitée à la consultation du fichier des cartes d'identité, du fichier des cartes volées et du fichier des personnes recherchées.

L'avant-projet de loi que s'apprête à présenter le gouvernement remet subrepticement en cause ces garanties. Si le principe de liberté de preuve restait affiché, ce ne serait qu'à défaut de détention d'une pièce d'identité sécurisée, passeport ou carte d'identité. Les modalités de preuve de l'identité seraient ainsi graduées et non plus à égalité. Le discours du ministre de l'Intérieur ne laisse guère de doute sur la perspective qui est ouverte : il souhaite qu'à terme (lorsque l'appareil de production le permettra) la carte d'identité soit obligatoire. Le couplage de fonctionnalités diverses, vécues comme « commodes » par les usagers, avec cet outil purement policier que constitue la carte d'identité, constitue une manière de la rendre indispensable et, de fait d'en généraliser la détention. Même si juridiquement la carte ne devenait pas obligatoire, les récalcitrants risqueraient inéluctablement de se trouver relégués au rang de citoyens de seconde zone.

La généralisation de la carte d'identité répond à la volonté de banaliser les contrôles. Il est annoncé que la carte sera « dans un premier temps bimode ». La consultation des données d'identité contenues dans la puce par les agents de contrôle se fera sans contact, alors que l'utilisation des autres fonctionnalités se fera par l'intermédiaire d'un lecteur et d'un code secret. Les prémisses d'un contrôle d'identité purement mécanisé et d'un contrôle à l'insu du porteur sont ainsi posées. La banalisation du contrôle, modalité d'imposition du pouvoir de l'État, et plus spécialement de la police, sur les citoyens est ainsi organisée.

Un fichier de police à l'échelle d'une population

Pour être infalsifiable, la nouvelle carte d'identité comportera des éléments dits « biométriques », sous forme numérisée. Au prétexte d'interdire des usurpations d'identité (une personne tentant de se faire remettre plusieurs titres sous des identités différentes), les données biométriques numérisées feront l'objet d'un nouveau fichage. Il existe déjà depuis 1987 un fichier national unique des cartes d'identité qui comporte non seulement les données d'état civil et les informations relatives à la délivrance du titre, mais l'adresse des détenteurs de carte. Il n'est toutefois pas obligatoire d'informer l'administration en cas de changement d'adresse. La perspective de généralisation de la carte d'identité permettra de compléter ce fichier pour en faire un fichier exhaustif de la population française. La logique, déjà contestée lors de la création de la carte d'identité sécurisée actuelle, compte tenu du risque inhérent au détournement d'un tel fichier de population par un État qui perdrait ses repères démocratiques, est donc encore accentuée.

S'y ajoute encore la constitution d'un fichier exhaustif d'empreintes digitales. Si la délivrance de la carte d'identité s'accompagne actuellement d'une prise d'empreinte, celle-ci

ne fait l'objet d'aucune numérisation, ni de la constitution d'un fichier. L'empreinte est conservée dans le dossier « papier » de délivrance du titre. Elle ne peut être consultée judiciairement que pour la rapprocher avec les empreintes d'une personne se prévalant de l'identité à laquelle elle se rapporte. Elle ne permet donc pas l'identification d'une empreinte ou d'une trace anonyme. Il n'est possible de procéder à ce type d'identification que par l'intermédiaire du fichier automatisé des empreintes digitales (FAED). La logique de ce fichier est toutefois totalement différente d'un fichier général de population puisqu'il ne réunit que les empreintes de personnes limitativement énumérées, mises en cause judiciairement. INES révèle ici sa véritable nature : il s'agit d'abord d'un projet à usage policier, qui relègue chacun au statut de suspect.

La création d'une base de données dactyloscopique de plusieurs dizaines de millions d'individus, aura pour effet d'exposer un nombre d'individus beaucoup plus important qu'actuellement à un risque d'identification et de suspicion erronée. L'empreinte digitale est en effet revêtue dans notre imaginaire commun d'une vertu d'infailibilité qui n'est pas réelle. Tous les dispositifs d'identification par les empreintes, quelle qu'elles soient, par comparaison d'une trace anonyme à une base d'empreintes, reposent sur un calcul de probabilité, de sorte que le risque d'erreur est d'autant plus grand que la base de données est importante. Le risque augmente encore lorsque la trace anonyme est incomplète ou imparfaite. L'identification erronée par le FBI et le placement en détention provisoire de Brandon Mayfield, à partir d'une trace papillaire relevée sur les lieux des attentats du 11 mars 2004 à Madrid a fourni une bonne illustration de ce risque. Ainsi, sauf à légitimer les pratiques policières et judiciaires qui tendent à se banaliser, consistant à jeter un filet sur des personnes a priori suspectes dont on élargit progressivement le cercle, le choix d'une base de données trop large n'apparaît pas réellement pertinent, même d'un point de vue strictement policier.

De l'interconnexion des fichiers au traçage

La banalisation du recours aux identifiants biométriques constitue sans doute un des enjeux les plus importants du projet INES.

INES propose de recourir à ce moyen d'identification pour des applications dont les enjeux sont sans commune mesure, au mépris du principe de proportionnalité : identification à visée sécuritaire d'une part, identification pour des applications administratives ou commerciales en ligne de l'autre. Le recours à une modalité d'identification hautement intrusive du point de vue de la vie privée, et hautement sécurisée, ne se justifie pas pour des applications banales pour lesquelles des systèmes d'identification et d'authentification existent déjà actuellement. Là encore, la proposition INES est sous-tendue par une logique de suspicion de fraude généralisée. On peut cependant rappeler que jamais le contrôle de l'identité du co-contractant n'a constitué une démarche habituelle du point de vue du droit des contrats.

Cette généralisation et cette banalisation du recours à la biométrie conduisent à une remise en cause d'une notion d'identité essentiellement déclarative (l'état civil), basée sur la confiance et la reconnaissance mutuelle et sociale. La bio-

métrie au contraire tend à fonder une identité réifiée et intangible, à laquelle l'individu ne peut accéder lui-même et à laquelle il ne peut se soustraire. La généralisation d'un tel système d'identification, et la création d'un véritable état civil parallèle sous la forme du fichier central des données biométriques, renforce considérablement les modalités d'exercice du pouvoir de l'État sur les citoyens.

L'équilibre né de la première loi informatique et libertés de 1978 et des avis de la Commission nationale de l'informatique et des libertés (CNIL), notamment l'interdiction de l'interconnexion des fichiers informatiques et la limitation du recours à un identifiant unique se trouve aussi gravement mis en cause. Les éléments biométriques utilisés pour l'identification sur les réseaux informatiques constituent un identifiant unique nouveau qui permettra a posteriori le traçage de l'ensemble des transactions effectuées par un même individu et leur rapprochement. Il s'agit là encore d'un nouvel outil de contrôle policier, qui s'inscrit au surplus dans un contexte à la fois de renforcement des pouvoirs d'accès de la police aux systèmes informatiques dans le cadre de ses investigations (loi sur la sécurité intérieure « LSI », et loi dite « Perben II ») et de diminution des pouvoirs de la CNIL, qui a perdu la faculté de s'opposer à des traitements décidés par décret en Conseil d'État sur, entre autres, des « données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes » (nouvelle loi informatique et libertés d'août 2004, article 27-I).

Le projet de carte électronique à données biométriques comporte ainsi des risques importants d'atteintes à la vie privée et aux libertés individuelles, alors que la réalité des objectifs affichés pour le justifier n'est pas démontrée. La conformité d'un tel projet au principe de proportionnalité apparaît donc inexistante, alors qu'il entretient par ailleurs une confusion illégitime entre des objectifs d'ordre régaliens et d'autres, d'ordre purement mercantile. Aucune garantie réelle ne permet de prémunir les citoyens contre une autorisation élargie de l'accès au fichier par les services de police publics et privés et le commerce des informations entre ces services.

Loin de correspondre effectivement à un élément de simplification de la vie administrative du point de vue de l'utilisateur, la carte d'identité électronique entérine une logique de suspicion généralisée qui ne pourra aller qu'en s'accroissant, saisissant toutes les opportunités ouvertes par les évolutions technologiques. Les mêmes arguments qui justifient aujourd'hui le recours à l'empreinte digitale et à la photographie, justifieront demain l'enregistrement de l'iris, de la rétine, voire de l'ADN. De même, la logique et la puissance d'une carte à puce multifonctions conduiront à la multiplication des applications sous prétexte de lutte contre la fraude, de sécurité, ou de commodité. La carte d'identité constituera un outil parfaitement intégré regroupant toutes les données personnelles d'un individu, au risque de le rendre parfaitement transparent pour l'État et pour ses partenaires institutionnels ou commerciaux les plus puissants.

À supposer démontrée la nécessité d'une plus grande sécurisation des titres d'identité d'une part et de l'autre des transactions informatiques, l'économie entière du projet doit être reconsidérée pour être limitée à ce qui est strictement nécessaire et pour que les finalités soient clairement identifiées et distinguées. En l'état, le projet INES doit être retiré.