IRIS
(Imaginons un réseau Internet solidaire)
294 rue de Charenton
75012 Paris
Tél/Fax+33(0)144749239
URLhttp://www.iris.sgdg.org
Emailiris-contact@iris.sgdg.org

INESun projet injustifié, nocif, et présenté suivant un procédé déloyal et antidémocratique

Position d'IRIS
27 avril 2005

[Ce document a constitué la trame de l'intervention d'IRIS dans le cadre du débat organisé par le FDI, à la demande du ministère de l'Intérieur, sur la CNIE et le projet INES (étape de Lille, 27 avril 2005), ainsi que de l'audition d'IRIS par la CNIL le 9 mai 2005]

IRIS considère le projet injustifié, nocif, et introduit suivant un procédé déloyal et antidémocratique. L'association se prononce donc contre ce projet et envisage des actions de sensibilisation aux dangers de ce projet et de mobilisation afin d'y faire échec.

1/ Le projet INES est injustifié

Les arguments du ministère de l'Intérieur ne sont pas convaincantsde la nécessité du projet

- Le ministère et le gouvernement sont **incapables de fournir des chiffres permettant de constater l'ampleur déclarée de la fraude** en termes de falsification de la carte d'identité actuelle, d'usurpation d'identité et de délivrance indue de titres multiples.

- Cette ampleur supposée de la fraude reste pourtant, à l'examen et selon les déclarations même des représentants du ministère, **le seul argument** servant à justifier la création d'une base de données centralisée comportant notamment des éléments biométriques.

*Eu égard à la teneur du projet, il y a donc là un **très fort risque d'atteinte au principe de proportionnalité**, principe cardinal de la législation française et européenne en matière de protection de la vie privée et des données personnelles.*

2/ Le projet INES est nocif

Malgré les déclarations du ministère de l'Intérieur visant à assurer que le projet permettra à la fois une sécurisation complète des informations et des garanties de limitation d'usage des données contenues dans la carte et dans la base de données centralisée, le projet ouvre la voie à de graves dérives

- La possibilité de **fichage généralisé** est patente, notamment par les choix suivants

- **Base de données centralisée**, contenant notamment des informations biométriques
- Le projet est conçu pour **plusieurs utilisations, dont la diversité dépasse la seule gestion de l'état civil**. Ces utilisations incluent les transactions avec des opérateurs privés, à travers le certificat de signature électronique
- Les techniques de biométrie choisies (face et empreintes digitales) sont justement celles qui laissent des traces, **traces qui de surcroît peuvent être collectées à l'insu de la personne concernée**, et donc sans son consentement (possibilité de photographie dans des lieux publics, relevé d'empreintes)
- Il est certain que **les utilisations des données biométriques contenues dans la carte et dans la base centralisée seront étendues au cours du temps**. Tout d'abord l'expérience l'a montré, notamment avec les fichiers STIC et FNAEG, et la réduction des pouvoirs de la CNIL par la refonte de la loi informatique et libertés ouvre la porte à des extensions d'utilisation par l'État sans accord de la CNIL. Ainsi, l'article 27-I nouveau de la loi N°2004-801 du 6 août 2004 permet d'autoriser, par décret en Conseil d'État, pris après avis motivé et publié – mais non nécessairement *conforme*□– de la CNIL qui perd ainsi la faculté de s'y opposer, des traitements sur, entre autres, des «□données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes□. Ensuite la question de la rentabilité économique du système se posera tôt ou tard, et l'accès automatisé aux données biométriques, par des acteurs privés (banques, commerces, etc.) ou par des acteurs publics pour la délivrance de certains droits, interviendra comme une réponse possible. Il existe de toutes façons déjà dans le commerce des lecteurs d'empreintes digitales, y compris destinés à des utilisations individuelles, comme par exemple en tant que substitut au contrôle d'accès par mot de passe à certains logiciels (courrier électronique, etc.).
- Le **choix d'une puce à lecture sans contact** entraîne des risques de lecture non autorisée (*skimming*) et d'interception indue des données transmises de la puce au lecteur sans contact (*eavesdropping*). Notons à cet égard que, pour citer cet exemple, le gouvernement américain subordonne la mise en oeuvre du passeport à puce sans contact pour ses ressortissants à l'obtention de la garantie que tous les risques de cet ordre peuvent être écartés (déclaration de Frank Moss, représentant du Département d'État US à la conférence CFP à Seattle le 13 avril 2005). De plus, il n'y a pas de justification impérative à la lecture sans contact, l'argument avancé de «□limitation de l'usure de la carte□ étant dénué du minimum de sérieux que l'on pourrait attendre du ministère de l'Intérieur.

- Les décisions qui seront prises pour la carte d'identité nationale seront, par le fait qu'elles concernent l'ensemble de la population, **des décisions structurantes**. Elles vont d'une part **structurer tous les choix ultérieurs en matière de mode de vérification d'identité**, que ce soit pour des besoins publics ou privés, fussent-ils aussi quotidiens qu'une opération de retrait de courrier postal recommandé ou de présentation d'un chèque bancaire à une caisse de supermarché. Elles vont d'autre part **structurer l'ensemble du marché de la biométrie et la sécurisation des transactions**, qu'il s'agisse des infrastructures, des matériels ou des logiciels. Ce marché est énorme et, de l'avis de tous les acteurs industriels, encore seulement en émergence.

- La mise en oeuvre du projet induira **une banalisation de l'usage de la biométrie**, et va forger le consentement de la population à se soumettre à des atteintes de plus en plus invasives à la vie privée. L'usage de la biométrie constitue pourtant un véritable changement d'échelle, puisque ces techniques permettent « la mesure et la reconnaissance de **ce que l'on est**, à la différence d'autres techniques de mêmes finalités, mais permettant de mesurer ou vérifier **ce que l'on possède** (carte, badge, document, ...) ou **ce que l'on sait** (mot de passe, code pin, ...) [cf. présentation à la conférence internationale des autorités de protection des données, Paris, 24 septembre 2001, http://www.paris-conference-2001.org/fr/Contribution/marzouki_contrib.pdf]

*Tout cela induit **un très fort risque d'atteinte au principe de finalité**, autre principe cardinal de la législation française et européenne en matière de protection de la vie privée et des données personnelles.*

3/ Le procédé est déloyal et antidémocratique

La façon dont le projet est présenté **vise à cacher à la population l'ampleur du risque**, afin d'obtenir son consentement par un processus de légitimation du projet et de ses objectifs, y compris par la diffusion d'informations inexactes. De surcroît, les décisions s'avèrent être prises à un niveau de détail très avancé et les négociations avec les communes, notamment à travers des discussions avec l'association des maires de France (AMF) sont déjà en cours pour déterminer combien de communes disposeront des dispositifs matériels et de l'infrastructure nécessaire au déploiement du projet. Cela montre bien que **les détails de mise en oeuvre du projet sont déjà en cours d'adoption,** alors même qu'un « débat public » se déroule (organisé par le FDI sur mission du ministère de l'Intérieur), que la CNIL n'a pas encore été saisie pour avis, et que le projet de loi n'a pas été transmis au Parlement, l'avant-projet n'ayant même pas encore été adopté en Conseil des ministres.

- **Il est faux de prétendre que le projet est dicté par des obligations internationales**. Les standards élaborés par l'OACI et le règlement européen du 13 décembre 2004 ne concernent que les passeports et documents de voyage. De plus, le standard de l'OACI est restreint à un seul élément biométrique, la photographie. Notons également que le règlement européen a été adopté par le Conseil des ministres comme une extension des accords de Schengen, et n'a donc pas de ce fait le même statut que d'autres documents communautaires. Enfin, les deux document (OACI et règlement européen) sont sujets à caution démocratique par leurs modes de discussion et d'adoption (voir à cet égard deux documents dont IRIS est signataire : la lettre ouverte adressée en mars 2004 à l'OACI par les ONG American Civil Liberty Union et Privacy International et la lettre ouverte adressée en novembre 2004 au Parlement européen par les ONG Privacy International, Statewatch et European Digital Rights – fédération européenne dont IRIS est membre : http://www.iris.sgdg.org/info-debat/comm-lettre-oaci0304.html et http://www.iris.sgdg.org/info-debat/comm-biometrie1104.html).

- **Il est faux de prétendre que la France n'aurait aucune responsabilité dans l'adoption de ces documents, et n'aurait pour ainsi dire « pas de choix autre que de s'exécuter »**. Par son suivi des développements européens et internationaux, notamment avec ses partenaires de la fédération EDRI et ses partenaires ONG américaines, IRIS a pu montrer à plusieurs reprises que la France joue un rôle moteur parmi ses partenaires européens et internationaux dans l'adoption de réglementations internationales portant gravement atteinte à la vie privée et à la protection des données

personnelles. Cela illustre bien le phénomène de « blanchiment de politique », également dénoncé par d'autres ONG européennes et américaines au vu des pratiques de leurs gouvernements respectifs.

- **La présentation du projet par le ministère de l'Intérieur entraîne la confusion par le mélange des genres**. Le projet serait destiné, outre l'état civil, à la fois et en vrac à la lutte contre le terrorisme, à la lutte contre l'immigration illégale, à la signature électronique pour les transactions administratives (administration électronique, alors même que le projet ADELE est développé par ailleurs) comme pour les transactions commerciales, à la mise en place d'une sorte de « guichet unique » facilitant les relations avec l'administration, et même à des utilisations individualisées au moyen d'un « portfolio personnel ».

- **La décision de rendre la carte obligatoire et payante a été officiellement annoncée**. Le constat que son caractère obligatoire n'avait pas eu cours depuis le régime de Vichy se passe de tout autre commentaire. Le fait de la rendre payante introduit un caractère discriminatoire et une rupture d'égalité des citoyens devant la loi.

4/ Caractéristiques d'une alternative acceptable pour IRIS

IRIS ne considèrerait comme acceptable qu'une alternative au projet actuel INES présentant les caractéristiques suivantes :

- **Finalités et usages :**
  - ⇨ La carte nationale d'identité doit uniquement permettre d'authentifier le porteur (la personne est bien celle qu'elle prétend être), à l'exclusion de toute possibilité d'identification d'un individu anonyme parmi une population
  - ⇨ La carte ne doit pouvoir faire l'objet d'aucune autre utilisation. Les certificats de signature électronique et autres utilisations individuelles, volontaires ou non, doivent être complètement dissociés de la carte nationale d'identité, de son support et de sa gestion.
  - ⇨ Si la carte doit comporter une puce, celle-ci ne doit servir qu'à authentifier la carte comme étant un document non falsifié (par exemple par signature électronique de l'autorité délivrant la carte)

- **Données contenues dans la carte et dans les fichiers d'état civil :**
  - ⇨ La carte ne doit comporter aucun élément biométrique
  - ⇨ La photographie du titulaire de la carte ne doit pas figurer sous forme numérisée dans la puce, mais uniquement de manière visible sur la carte pour identification par un contrôleur humain
  - ⇨ Il ne doit pas y avoir de constitution de base de données centralisée

- **Modalité d'accès aux données contenues dans la carte :**
  - ⇨ Si la carte doit comporter une puce pour l'authentification du document, la lecture de cette puce ne doit pas se faire sans contact

- **Caractère obligatoire et coût :**
  - ⇨ La carte doit demeurer non obligatoire et doit continuer d'être délivrée gratuitement.