Commission Nationale de l'Informatique et des Libertés

Note de la Direction de l'Expertise informatique et des Contrôles

Objet : Traité de Prüm & annexe technique et administrative pour sa mise en application

Note établie sur le document « Decision of the Committee of the Ministers concerning the Treaty of Prüm
réf draft document ATIA REV 5 -10th July 2006

Pour éviter des répétitions, cette note d'expertise s'est principalement focalisée sur l'ADN mais ses conclusions sont également valables pour les données dactyloscopiques (empreintes digitales)1.

Le cas des registres d'immatriculation de véhicules est plus simple puisqu'il n'y a pas dédoublement de la base de données.

A. Qui fait quoi et où ?

Le traité stipule :

a) Dans son article 2, alinéa 2, le principe de l'éclatement en 2 bases de données distinctes entre d'une part les données biométriques (les « profils ADN ») et d'autre part les données textuelles d'identification des individus.

   Pour un individu donné, le passage de la première base vers la seconde se fait par l'intermédiaire d'un index qui ne peut être obtenu que si la recherche dans la première base s'est révélée positive.

b) Dans son article 3 alinéa 2 :

   «Si … une concordance entre un profil ADN transmis et un profil enregistré dans le fichier de la Partie contractante destinataire est constatée, le point de contact national ayant lancé la consultation… »

c) Des dispositions analogues pour les données dactyloscopiques (empreintes digitales) : cf Article 8 et article 9 alinéa 2.

d) Par contre, pour les registres d'immatriculation des véhicules, il est prévu un accès direct aux fichiers nationaux, c'est à dire qu'il n'y pas de dédoublement du fichier : article 12.

e) A l'article 15 :

1 L'annexe B1 qui founit un ensemble d'informations détaillées sur les données dactyloscopiques est absente du document intitulé « Decision of the Committee of Ministers , REV5» qui a constitué la matière première de la présente expertise, mais cela ne devrait pas remettre en cause les conclusions de cette note.

« Chaque Partie contractante désigne un point de contact national pour la transmission de données en vertu des articles 13 et 14 » (ces 2 articles traitent respectivement de la « Transmission de données à caractère non personnel » et de la « Transmission de données à caractère personnel »).

Sur le plan opératoire, ces stipulations se traduisent par l'obligation d'exécuter en 2 étapes les consultations faites à partir de profils biométriques comme l'ADN ou les empreintes digitales.

1) D'abord une première étape de comparaison avec la base de donnée biométrique sur le critère d'un profil ADN ou dactyloscopique

2) Puis, en cas de résultat positif, grâce à l'index fourni à l'issue de la première étape, une consultation de la deuxième base de données contenant les informations textuelles sur les identités des individus.

Recommandation 1

Ce scénario de consultation en deux temps à partir d'un profil biométrique exclut que les étapes 1) et 2) puissent être enchaînées automatiquement car le principe de la séparation en 2 bases de données stipulé par le Traité dans son article 2 serait alors détourné.

Sur ce point, l'annexe A.3 est conforme à la disposition du Traité car il prévoit une intervention humaine entre les deux étapes, à savoir un « DNA expert », cf le 1er paragraphe de la page 21/47. Mais il faut attendre la lecture de la dernière page de cette annexe pour rencontrer l'expression « DNA expert ».

- Le Traité s'est donné la peine dans son article 2 de stipuler le principe de la séparation. **Dès lors, il paraît logique que ce principe soit réaffirmé dans le corps principal du document anglais "Decision of the Committee of Ministers", en stipulant l'intervention obligatoire d'un "DNA expert" ou d'un "Fingerprint expert" entre les 2 étapes d'une consultation. La présence du « DNA expert » du "Fingerprint expert" pourrait également être réaffirmée dès la première page de l'annexe A.3 quand sont décrites les 2 étapes « 1st step ... 2nd step.. »**

- D'autre part, voir notre recommandation 7 ci-dessous destinée à assurer la traçabilité de l'intervention de cet expert.

Qui est en charge du déclenchement des étapes 1) et 2) d'une consultation ?

La lecture combinée de l'article 15 (cf le point e) ci-dessus) et du 2ème alinéa de l'article 3) (cf le point b) ci-dessus) du Traité indique que la première étape d'une consultation sur critère biométrique est exécutée par le point de contact national : « *le point de contact national ayant lancé la consultation…* »

Quant à la deuxième étape, rien n'est précisé dans le Traité ; Toutefois, la logique de la séparation en deux bases de données distinctes est de ne réserver l'accès à la base des

données d'identification textuelles des individus (c'est à dire la deuxième étape d'une consultation) qu'à travers une structure exclusive constituée ad-hoc.

- Ainsi, notre analyse est que les deux étapes d'une consultation à partir d'un profil biométrique devront être exécutées au sein du point de contact national ou du moins sous sa responsabilité.

- Quant aux consultations des registres nationaux d'immatriculation des véhicules, l'article 12 est explicite : c'est le point de contact national qui est en charge de cette mission.

Or, le document « Decision of the Committee of Ministers, REV5 » n'est pas clair sur ce sujet.

Son point 3.2 page 4/47 évoque « a set of common specifications, including matching rules, algorithms and Parties code numbers". Mais il n'y est pas fait mention des équipements (terminaux de consultations, réseau) ni des personnels chargés de procéder aux consultations. Sauf indirectement, au point 4.3 : « the answer to the query… will be sent to the national contact point".

L'annexe A.3, pages 16/47 à 21/47, qui décrit abondamment les 2 étapes d'une consultation à partir d'un profil ADN, ne donne pas plus d'informations sur le sujet des personnels et des équipements.

Recommandation 2

Sur le plan de l'analyse des sécurités, il faudrait que le document « «Decision of the Committee of Ministers » **soit plus explicite sur le statut des personnels qui seront en charge des consultations (et de facto également, sur les équipements, terminaux de consultation et réseau)**

Recommandation 3

L'annexe A.3 contient une erreur ou une ambigüité. Elle laisse ouverte la possibilité d'un traitement par lot (cf 2ème paragraphe en haut de la page 17 « The definition of needs regarding a mechanism **for batch processing exchanges** will be studied later ».

L'expression « **Procedures by batches** » est également utilisée dans le titre du point 3.1 page 17/47.

Or l'article 3 du Traité, fin de l'alinéa 1, stipule que « La consultation ne peut s'opérer **qu'au cas par cas** …».

Il faudrait que la portée de ce « batch processing » soit mieux définie afin de s'assurer qu'il ne contrevient pas à l'article 3 du Traité.

B. Pour une meilleure authentification et traçabilité.

Il est indiqué au point 4.1 page 4, que lors de la première étape d'une consultation sur critère biométrique, la Partie contractante requérante ("requesting Party") soumet sa requête au moteur de recherche ("automated search or comparison") d'une Partie contractante destinataire ("Requestet party") en lui fournissant les informations suivantes :

- Le code identification de la Partie contractante requérante,
- La date, l'heure et le numéro d'ordre de la requête ("reference number of the query")
- Le "DNA profile" objet de la recherche
- Le type de "DNA profile" : "crime scene DNA profil" (2.8 individu non identifié) ou "Reference DNA profile" (2.9 individu identifié)

Recommandation 4

Par rapport à la liste ci-dessus, dans le souci d'assurer une meilleure traçabilite et authentification de l'organisme requérante lors de la première étape d'une consultation :

- La fourniture du seul code d'identification de la Partie contractante requérante est insuffisante, **il faudrait ajouter le code identifiant de l'agent (au sein du point de contact) qui procède à la consultation**.

- Au point 2.17 page 3/47, est prévue l'information « motif de la consultation » ("reason for search or supply of data means"). **Il serait grandement souhaitable que cette information figure parmi celles à fournir lors de la soumission de la requête**.

- **Pour authentifier de façon certaine l'émetteur de la requête, l'ensemble des informations fournies *(les 4 initialement prévues complétées par les 2 informations ci-dessus)* devrait être signé électroniquement par la Partie requérante lors de la soumission de sa requête.**

Comme résultat de la première étape d'une consultation, la Partie contractante destinataire (« requested Party ») renvoie une réponse composée des informations énumérées au point 4.3, page 4/47.

Recommandation 5

Pour assurer la confidentialité et l'authenticité des résultats renvoyés par la Partie contractante destinataire à l'issue de la première étape d'une consultation sur critère biométrique :

- **L'index (la donnée 4.2.4 page 4/47) contenu dans le résultat de la recherche devrait être chiffré**, car la logique de l'éclatement sur 2 bases de données distinctes stipulée par l'article 2 du Traité implique que le passage de l'une des bases à l'autre soit extrêmement encadré, l'index utilisé ne devrait donc pas être révélé. Il n'y aurait pas de problème de partage de connaissance de la clef de chiffrement/déchiffrement car c'est la même Partie destinataire et elle seule qui aura à procéder au déchiffrement lorsque lui sera demandée l'exécution de la 2ème étape..

- **L'ensemble des données composant le résultat devrait être signé électroniquement par la Partie contractante destinataire pour en garantir l'authenticité**.

Le document ATIA Rev 5 n'explicite pas, y compris dans son annexe A.3 (point 5, page 21/47), les informations qui devront être fournies par la Partie contractante requérante pour enclencher la deuxième étape de la consultation.

Recommandation 6

Pour assurer une meilleure traçabilité et authentification des requêtes soumises lors de la 2ème étape d'une consultation sur critère biométrique, la Partie contractante requérante devrait fournir au minimum

a) **Le code identification de la Partie contractante requérante,**
b) **Le code identification de l'agent (au sein du point de contact) qui procède à la consultation.**
c) **La date, l'heure et le numéro d'ordre de la requête**
d) **Le résultat obtenu à l'issue de la première étape de la consultation (cf l'encadré ci-dessus).** ***Rappelons que ce résultat contient l'index permettant au moteur de recherche de la 2ème étape de procéder à la consultation de la base de données. Ce résultat étant signé électroniquement (si notre recommandation 5 est retenue), le moteur de recherche de la 2ème étape a la garantie que sa recherche est synchrone avec un résultat positif obtenu à l'issue d'une première étape de consultation.***
e) **voir également la recommandation 7 ci-dessous pour une éventuelle signature électronique du DNA-Expert ou Fingerprint-Expert.**
f) **Le tout devrait être signé électroniquement par la Partie contractante requérante pour authentifier la requête.**

Recommandation 7

Pour acter l'intervention du DNA -Expert ot du Fingerprint-Expert entre les 2 étapes d'une consultation sur critère biométrique et en assurer sa traçabilité, **il faut introduire la signature électronique de cet expert.**

- Soit l'organisation du point de contact national est telle que c'est l'expert lui-même qui procède à la soumission de la 2ème étape de la consultation, auquel cas, la recommandation 6 suffit pour acter son intervention puisqu'elle prévoit la signature électronique du soumissionnaire de la requête.

- Soit l'expert au sein du point de contact national n'intervient pas dans la soumission des requêtes informatiques, auquel cas la liste des informations énumérées dans la recommandation 6 doit être complétée par :

  L'information d) doit être signée électroniquement par l'expert et le résultat incorporé en tant qu'élément d'information e) dans la liste des informations à fournir énumérées dans la recommandation 6.

Recommandation 8

Pour garantir l'authenticité du résultat obtenu à l'issue de la 2ème étape d'une consultation sur critère biométrique (ou de l'unique étape s'il s'agit de consulter un fichier d'immatriculation de véhicules):

- **Le résultat devrait être signé électroniquement par la Partie destinataire pour en garantir l'authenticité**.

- Par contre, il ne semble pas utile que ce résultat soit envoyé chiffré

C. La procédure de comparaison proprement dite exécutée par le moteur de recherche sur un profil ADN.

Le principe de la recherche dans la base de données biométrique ADN est décrit dans l'Annexe A, pages 12 à 14/47.

La recherche se fait par comparaison sur 24 segments (loci) d'ADN parmi lesquels 7 constituent le standard européen (ESS/ISSOL).

- Une consultation est déclarée entièrement positive ("full match") s'il y a égalité sur les 7 segments d'ADN (loci) du standard européen ESS/ISSOL

- Une consultation est déclarée partiellement positive ("near match") s'il y a égalité sur seulement 6 des 7 segments du standard européen ESS/ISSOL.

- En dessous de 6 égalités parmi les 7 segments du standard européen ESS/ISSOL, la consultation est déclarée négative.

- Outre les 7 segments d'ADN du standard européen, la base de données peut contenir 17 autres segments (loci) d'ADN qui ne sont utilisés par le moteur de recherches que s'il y a eu préalablement un résultat positif ("full" ou "near") sur les 7 segments appartenant au standard européen ESS/ISSOL, afin de renforcer, s'il y a égalité sur certains des 17 autres, la validité du résultat déclaré positif.

Dans un profil d'ADN utilisé comme critère de consultation, certaines positions peuvent être occupées par le caractère « Wild card » ou « joker » c'est à dire ayant une valeur indéterminée (cf haut page 13/47)

Recommandation 9

L'usage du caractère « joker » (et également la notion de « micro-variant », cf page 13) dans un profil d'ADN utilisé lors de l'exécution d'une requête de recherche laisse perplexe.

Toutefois, l'auteur de cette note n'étant pas expert dans ce domaine et le document ATIA Rev 5 mentionnant le protocole mis en œuvre par Interpol (« »DNA-procedures of Interpol », bas de la page 12/47), **il faudrait tout du moins que ce document précise que la totalité de l'algorithme décrit dans l'annexe A.1 fait partie des protocoles standards utilisés dans les services de police.**