2ème JOURNEES NATIONALES DE INFORMATIQUE ET DES LIBERTES

Thème:

« L'usage de la biométrie au BENIN et ses enjeux vis-à-vis de la protection des libertés fondamentales. »

Palais des Congrès, Cotonou le 05/08/2015

Présenté par : Emmanuel ZOSSOU - Ingénieur informaticien

Commissaire à la CNIL-BENIN - Responsable du Secteur des TIC,

Cyber Sécurité & Relations Internationales

Sommaire

1. Définition et concept de la biométrie

QU'EST CE QUE LA BIOMETRIE ?

☞Le mot biométrie signifie « mesure + vivant » ou « mesure du vivant ».

☞ Il existe 3 possibilités pour prouver son identité :

1. Ce que l'on **possède** (carte, badge, document) ;
2. Ce que l'on **sait** (un nom, un mot de passe) ;
3. Ce que l'on **est** (empreintes digitales, main, visage…) : la **biométrie**.

☞La biométrie est une technique d'**identification**

1. **Analyses biologiques** : Odeur, sang, salive, urine, ADN…
2. **Morphologie** : son œil, son empreinte digitale, sa voix,
3. **Comportement** : sa signature, sa façon d'écrire etc.

POURQUOI UTILISER LA BIOMETRIE ?

Plusieurs raisons peuvent motiver l'usage de la biométrie :

✓**Confort** - l'ouverture d'une session dans un système informatique : **Identification** aisée.

✓**Sécurité** - les empreintes digitales un moyen d'**authentification** fiable connu.

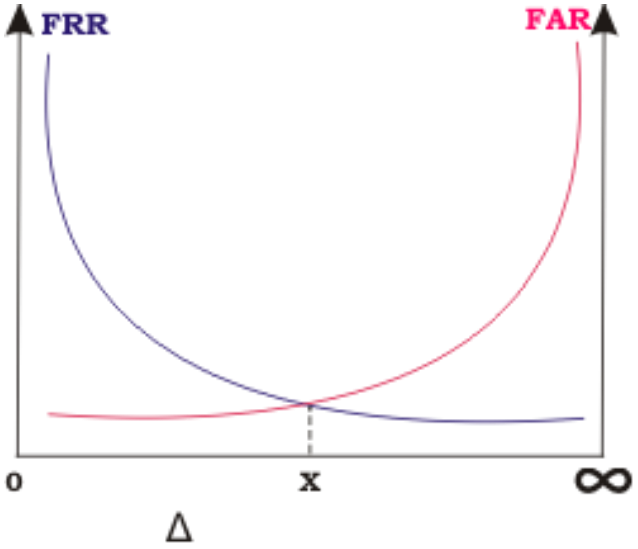
✓**Une haute sécurité** - en l'associant à d'autres technologies comme le cryptage, la carte à puce…

AVANTAGES ET INCONVENIENTS DE LA BIOMETRIE

La biométrie présente malheureusement un inconvénient majeur; en effet aucune des mesures utilisées ne se révèle être totalement exacte.

Les fabricants de dispositif biométrique ne recherchent nullement la sécurité absolue, ils veulent quelque chose qui fonctionne dans la pratique.

Un système sûr aura un FAR le plus bas possible. Dans la vie courante, les industriels cherchent principalement à avoir un compromis entre ces 2 taux, FRR et FAR, qui sont eux liés suivant une relation illustrée ici :



Légende :

FRR : False Rejection Rate
FAR : False Acceptation Rate

Exemple de vulnérabilité : le cas des empreintes digitales

Les empreintes digitales représentent sans aucun doute les données biométriques les plus couramment utilisées. Mais, Là encore, il convient de ne pas se laisser impressionner par une image illusoire de haute technologie, produit miracle.

- Empreinte abimée irrémédiablement suite à des travaux manuels.

- Cas d'attaque les bases de données de référence.

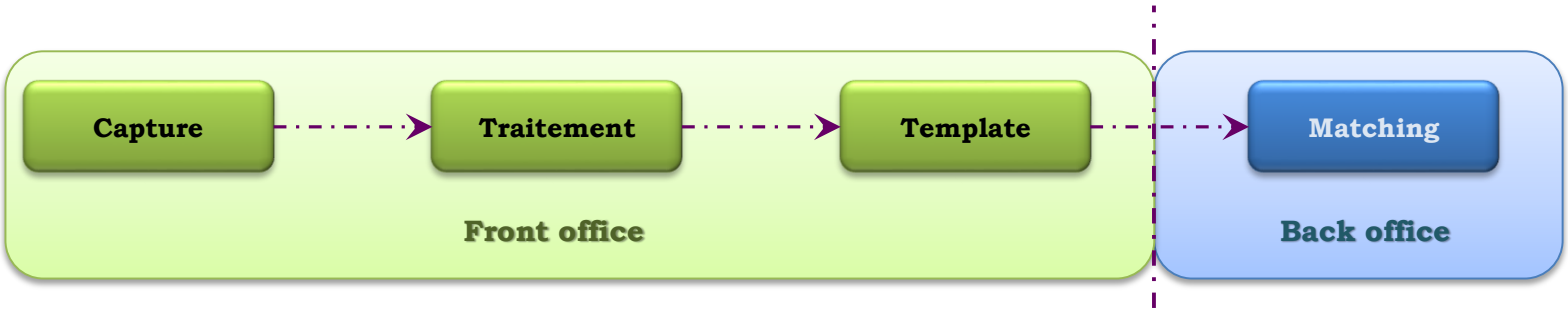
COMMENT FONCTIONNE LA BIOMETRIE ?

Les étapes du traitement biométrique sont :

- **Capture** de l'information à analyser (image ou son).

- **Traitement** de l'information et création d'un fichier " signature/gabarit " (éléments caractéristiques de l'image), puis mise en mémoire de ce fichier de référence sur un support (disque dur, carte à puce, code barre).

- Dans la phase de **vérification**, l'on procède comme pour la création du fichier " signature/gabarit " de référence, ensuite on compare les deux fichiers pour déterminer leur **taux de similitude** et prendre la décision qui s'impose.



Exemple: cas de l'empreinte digitale

La donnée de base dans le cas des empreintes digitales est le dessin représenté par les crêtes et sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu.

Une empreinte complète contient en moyenne une centaine de ces points caractéristiques (les "minuties").

Image d'origine

Image binarisée

Extraction des minuties

Les informations stockées ne sont en principe jamais les images d'origine, mais un modèle mathématique appelé un " gabarit " ou " template " .

On estime qu'il y a plus de cent points de convergences entre deux empreintes identiques. En France, la loi exige 12 points (appelés minuties) relevés sans contrariété pour authentifier l'empreinte d'un suspect. Entre 8 et 10 points, une forte présomption est établie grâce à des algorithmes. On utilise des algorithmes basés sur le théorème de Poincaré-Hopf pour extraire les minuties.

Comparaison des minuties :

- ✓**Match > 12** : Identification certaine
- ✓**8 < Match < 12** : Décision du groupe d'expert
- ✓**Match < 8** : Identification rejetée

La probabilité que deux personnes aient la même empreinte digitale est de 1 sur 10^{14}, ce qui est très faible à l'échelle de la population humaine.

2. Les enjeux

2.1 La problématique de l'introduction de la biométrie dans listes électorales au Bénin

2.2 Pertinence du choix et des moyens mis en œuvre au regard de la protection de la vie privée

2.1 La problématique de l'introduction de la biométrie dans listes électorales au Bénin

2.1. Problématiques des listes électorales biométriques

D'une manière générale, parmi les nombreux domaines d'applications de la biométrie, le processus électoral en a retenu essentiellement deux, celui de l'établissement des listes électorales et celui du vote.

Ce choix est fondé sur les difficultés liées à l'identification des électeurs au moment de leur inscription et au moment du vote.

Cela a engendré dans tous les pays de l'Afrique Francophone une problématique dans la gestion des processus électoraux.

Problématiques des listes électorales biométriques

Au Bénin comme dans la plus part des pays francophones, la fiabilité des listes électorales a été de façon récurrente au cœur de toutes les contestations électorales avec comme récriminations essentielles :

- l'inscription non exhaustive des électeurs ;
- l'inscription d'électeurs mineurs ou fictifs favorisée par le système de témoignage ;
- l'inscription multiple d'électeurs ;
- l'existence d'électeurs décédés sur les listes électorales.

Problématiques des listes électorales biométriques

Ces anomalies graves qui constituent des sources de fraudes ont fini par mettre en cause la fiabilité des listes électorales.

A l'analyse, elles puisent leur origine dans les défaillances du système d'état civil, incapable d'enregistrer tous les faits d'état civil à temps mais aussi de délivrer à tous les citoyens des documents authentiques les identifiant.

Même les opérations de recensement à vocation électorale avec des données alphanumériques et le système de témoignage n'ont pas apporté la solution.

Problématiques des listes électorales biométriques

D'où une ruée vers l'enrôlement biométrique considérée comme une panacée, une solution magique à tous les problèmes de transparence et de fiabilité électorales.

Ainsi notre pays s'est lancé dans les opérations d'enrôlement biométrique sans :

- une **étude consistante** de faisabilité ;
- **mesurer** les conséquences sur la vie privée;
- un cadre juridique approprié;
- …

2.2 Pertinence du choix et des moyens mis en œuvre au regard de la protection de la vie privée

Pertinence du choix et des moyens mis en œuvre au regard de la protection de la vie privée

Le Bénin a eu recours à la biométrie dans le but d'améliorer la qualité du processus électoral en renforçant sa transparence et la fiabilité de ses résultats.

L'introduction de la biométrie soulève sans nul doute des inquiétudes et suscite des interrogations sur la pertinence de ce choix, son efficacité, son coût et ses inconvénients sur la vie privée.

En effet, la collecte des données biométriques doit être entourée de multiples précautions compte tenu des risques qu'elle induit.

Des modalités particulières s'imposent lors de l'entreposage de ce type de renseignement sensible qui exige une attention particulière et des mesures de sécurité adaptées.

Pertinence du choix et des moyens mis en œuvre au regard de la protection de la vie privée

Les dispositions de la loi 2009 du 22 mai 2009 sont elles toutes respectées?

Considérant les risques liés à l'utilisation de la biométrie (par exemple : de vol permanent d'identité, de sécurité liée à la centralisation des bases de données, de sécurité des réseaux, de discrimination des personnes, de piratage des technologies, des limites de la technologie utilisée, etc.), quelles sont les mesures envisagées pour y faire face?

Comment sont informés les citoyens de l'ensemble des risques connus associés ou inhérents au système et à la technologie biométriques utilisés afin que leurs consentements soient éclairé?

La banque de données biométrique constituée a-t-elle été autorisée par la CNIL avant son utilisation?

Pertinence du choix et des moyens mis en œuvre au regard de la protection de la vie privée

Quelles sont les autres mesures de sécurité qui protégeront les données biométriques et assureront la sécurité et la confidentialité de ces données?

Le degré de sécurité envisagé par le responsable du traitement par l'utilisation de la biométrie est-il proportionnel aux risques ?

Une personne peut-elle accéder à ses données biométriques? Comment?

Les données peuvent-elles lui être communiquées de façon intelligible? Si oui, par quel mécanisme?

Une personne peut-elle exercer son droit à la rectification? Comment?

Pertinence du choix et des moyens mis en œuvre au regard de la protection de la vie privée

Peut-on réellement faire de la biométrie pour ses avantages pratiques tout en respectant 100% des vies privées en jeux ?

Face à toutes ces questions sans réponses actuellement il devient alors nécessaire, de doter le pays des moyens législatifs nouveaux et des moyens matériels conséquents, pour que le processus de garanti e et du respect de la vie privée ne retarde, ni ne bloque le développement des nouvelles technologies au Bénin.

Des compromis ne doivent-ils pas être trouvés pour éviter que l'un ne prenne le pas sur l'autre ?

CONCLUSIONS

On peut constater que la biométrie est une véritable alternative aux mots de passe et autres identifiants. Elle permet de vérifier que l'usager est bien la personne qu'il prétend être. Cette technologie est en pleine croissance et tend à s'associer à d'autres technologies comme la carte à puce.
Cependant la protection de la vie privée est aujourd'hui, un droit fondamental de l'homme et un impératif mondial

C'est un sujet incontournable dans tout pays démocratique.

C'est pourquoi , je pense personnellement que la CNIL devrait plaider pour la prise de nouvelles lois sur l'utilisation de la biométrie et l'inscription de la protection des données personnelles dans la Constitution, au titre des droits fondamentaux des citoyens.

Je vous remercie pour votre attention !

www.cnilbenin.bj

Emmanuel.zossou@cnilbenin.bj