LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES

PRINCIPAUTE DE MONACO

RAPPORT SUR LES DISPOSITIFS DE CONTROLE D'ACCES SUR LE LIEU DE TRAVAIL, MIS EN ŒUVRE PAR LES PERSONNES PHYSIQUES ET MORALES DE DROIT PRIVE

Avril 2011

SOMMAIRE

INTRODUCTION

Depuis quelques mois, la Commission de Contrôle des Informations Nominatives est de plus en plus souvent approchée aux fins d'autoriser la mise en place de dispositifs biométriques dans les entreprises et organismes de la Principauté.

En l'absence de dispositions légales, les responsables de traitements sont désireux d'obtenir un cadre juridique aux fins de se mettre en conformité avec les dispositions de la loi n° 1.165 du 23 décembre 1993, modifiée. Ils souhaitent être également guidés dans les choix des technologies s'y rapportant aux fins d'éviter d'engager des investissements parfois lourds et incompatibles avec les dispositions de la Principauté en matière de protection des informations nominatives et avec la Convention 108 du Conseil de l'Europe.

Pour ces raisons, la Commission de Contrôle des Informations Nominatives a souhaité rédiger le présent rapport, inspiré notamment des travaux du Conseil de l'Europe, afin d'attirer l'attention sur les spécificités de la biométrie.

En effet, la donnée biométrique n'est pas une donnée comme les autres : elle touche au corps humain et a une dimension indubitablement sacrée. Elle est incontestablement une donnée sensible au sens de la loi n° 1.165 précitée.

Les traitements biométriques sont soumis à l'article 11-1 de loi n° 1.165 dans les hypothèses suivantes :

- lorsque le traitement automatisé comporte des données biométriques nécessaires au contrôle de l'identité des personnes ; ou,
- lorsque le traitement automatisé en mis en œuvre à de fins de surveillance.

A ce titre, ces traitements sont soumis à l'autorisation de la Commission de Contrôle des Informations Nominatives.

Devant la pluralité des dispositifs biométriques existants et à venir, la Commission a souhaité, préalablement aux trois délibérations portant recommandations qui seront publiées au Journal de Monaco et citées dans le présent rapport, établir un certain nombre de principes inspirés des travaux du Conseil de l'Europe.

Elle ne s'est cependant pas cantonnée à transposer ces travaux, mais a également souhaité encadrer la biométrie telle qu'elle peut être concevable et acceptable en Principauté. La CCIN s'est ainsi efforcée d'opérer un arbitrage entre certaines biométries dites « *de confort* » et d'autres qui répondent à une réelle nécessité, de sorte à garantir le droit des personnes concernées sans entraver l'activité des entreprises qui font l'économie de la Principauté.

En effet, la Commission s'est attachée à prendre en considération les aspects géographiques de la Principauté, à assurer la sécurité des traitements biométriques et des informations qui s'y rapportent, et surtout à garantir le droit des personnes concernées par ces traitements.

Elle a souhaité par ailleurs que le présent rapport soit accessible à tous, aux entreprises et aux organismes désireux de recourir à la biométrie, aux responsables de traitements pour les guider dans leurs travaux, et à la population de la Principauté pour l'informer de ses droits.

I) Les enjeux et techniques de la biométrie

Il convient dans un premier temps de définir la biométrie et ses composantes avant d'en étudier ses procédés les plus répandus.

A. Le domaine de la biométrie selon le rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques

Ce rapport définie la biométrie comme un terme faisant « *référence à des systèmes qui utilisent des caractéristiques physiques, physiologiques ou des éléments de comportement personnel mesurables afin de déterminer l'identité ou de vérifier l'identité alléguée d'un individu* ». Cette définition synthétise plusieurs notions qu'il convient de développer.

En effet, à sa lecture, on comprend immédiatement que tous les systèmes biométriques n'analysent pas l'individu de la même manière. Il ya ceux qui « *utilisent des caractéristiques physiques ou physiologiques* » afin d'étudier des particularités morphologiques spécifiques, uniques, et le plus souvent permanentes (empreintes digitales, contour de la main, forme du visage, de la rétine, de l'iris de l'œil). Et il y a ceux qui analysent du comportement de l'individu (tracé de sa signature, l'empreinte de sa voix, sa démarche, sa frappe sur le clavier d'un ordinateur).

Néanmoins, quelque soit le système adopté, le but demeure identique : « *déterminer l'identité ou vérifier l'identité alléguée d'un individu* ». Il est intéressant de noter que la définition opère une distinction entre identification et vérification qui n'est pas sans conséquence à l'aune de la protection des données. Le choix entre ces deux « *fonctions* » de la biométrie dépend de la finalité envisagé du traitement automatisé.

La vérification procède de la comparaison d'un échantillon biométrique présenté avec les données biométriques enrôlées appartenant à une seule personne (« *one to one* ») ; il peut s'agir par exemple des empreintes digitales ou du contour de la main. Le résultat est positif ou négatif, et la comparaison est soit acceptée ou soit rejetée. Seules les données relatives à la personne concernée font l'objet d'un traitement automatisé.

Lors de l'identification, les données biométriques présentées ne sont pas seulement comparées à celle de la personne concernée, mais également avec celles d'autres personnes concernées (« *one to many* ») contenues dans la même base de données.

Il est constant que la collecte d'informations nominatives doit être proportionnée à la finalité du traitement : il faut donc vérifier si l'identification est absolument nécessaire. A défaut, la vérification lui sera préférée. En tout état de cause, lorsque l'on opte pour un système d'identification alors que l'on peut choisir un système de vérification, il faut pouvoir justifier ce choix par un intérêt spécifique.

Que le but soit d'identifier ou de vérifier l'identité alléguée, il existe un processus biométrique qui se décompose ainsi que suit.

Un échantillon biométrique est prélevé sur un individu, par exemple le relevé d'une empreinte digitale ou un balayage de l'iris. Cette caractéristique physique peut être représentée au moyen d'une image[1]. Toutefois, il arrive que des données soient extraites de

[1] Op. cit., p.5 ;

cet échantillon. Elles constituent le « *gabarit biométrique* ». Les données biométriques, qu'il s'agisse de l'image ou du gabarit, sont alors conservées sur un support de stockage.

Ces phases préparatoires constituent le « *processus d'enrôlement* ». La personne dont les données sont ainsi stockées est appelée l'« *enrôlé* ».

La finalité elle-même du système biométrique n'intervient qu'à un stade ultérieur. Lorsqu'une personne se présente au système, celui-ci va lui demander de présenter ses caractéristiques biométriques. Le système procédera alors à une comparaison entre l'image des données présentées (ou le gabarit extrait de ses données) et les données biométriques de l'enrôlé. Si la comparaison est positive, la personne sera reconnue et « *acceptée* » par le système. Si elle ne l'est pas, la personne ne sera pas reconnue et sera « *rejetée* »[2].

Les données biométriques ainsi récupérées sont issues du corps humain. Elles ont un caractère immuable qui permet le « *traçage* » des individus et leur identification quasi-certaine. On peut, en se basant sur cette notion de traçage, distinguer trois types de biométries :

- une biométrie « *à traces* » : cette catégorie recouvre les empreintes digitales et palmaires, dans la mesure où tout individu dépose des traces à son insu sur tous les objets qu'il touche. Les risques qui découlent de l'utilisation de ces techniques sont les possibles captures et reproductions de ces traces (fabrication d'un faux doigt par exemple) ;
- une biométrie « *sans trace* » : cette catégorie recouvre le contour de la main, le réseau veineux des doigts de la main ;
- une biométrie « *intermédiaire* » : cette catégorie recouvre la voix, l'iris de l'œil, la forme du visage. Elle ne doit pas être sous-évaluée. En effet, le niveau de fiabilité d'un procédé tel que la reconnaissance de l'iris de l'œil permet un niveau de traçabilité très élevé tant au regard de l'information que des possibilités de capture de celle-ci.

Cependant, si le traçage des individus permet une reconnaissance quasi-certaine, il faut avoir à l'esprit qu'« *une correspondance absolument parfaite entre les données enrôlées et celle présentées ensuite au système est techniquement impossible. L'utilisation d'un système basé sur des données biométriques repose inévitablement sur des probabilités d'ordre statistique* ».

En l'absence de certitude mathématique, le système se borne donc à reconnaître l'individu. Il se pose dès lors deux questions :

- celle de la normalisation quant à la technique biométrique utilisée et les caractéristiques des matériels utilisés ;
- celle du degré de confiance qu'il peut être accordé au procédé biométrique.

Le rapport d'étape susvisé soulève à cet égard quatre situations qui illustrent les limites de la biométrie dans son acception probabiliste :

- « *Un système de filtre est mis en place dans un stade afin d'endiguer le risque d'entrée de hooligans qui figurent sur une liste avec leur données biométrique. L'erreur du système profitera à l'indésirable qui pénétrera dans le stade ;*
- *Le même système reconnaît à tort un individu éligible à pénétrer dans le stade ;*
- *Un système de carte à puce servant de clé permettant de pénétrer dans des locaux sécurisés ne reconnaît pas à tort un individu autorisé. En l'absence de système alternatif ou supplétif, l'individu restera bloqué. L'importance d'une supervision*

[2] Op.cit., p.5.

humaine du système prend alors tout son intérêt pour palier aux errements du système ;

- *Le même système reconnaît à tort une personne non autorisée. La sécurité du lieu est menacée*[3] ».

Il faut donc admettre le caractère probabiliste des procédés biométriques et comprendre qu'aucun dispositif, même le plus sûr, ne peut faire figure de panacée en matière de sécurité. Il peut donc exister des limites dans ces systèmes de reconnaissances.

Il convient désormais de dresser une brève typologie des procédés biométriques.

B. Une brève typologie des procédés biométriques

Il ne s'agit pas ici de dresser la liste exhaustive des procédés biométriques existants mais d'étudier ceux les plus couramment utilisés.

a) L'empreinte digitale

Au chapitre des procédés biométriques les plus courants, la capture de l'empreinte digitale est sans doute celui le plus connu. Il a d'ailleurs largement contribué à attiser toutes les méfiances à l'égard de la biométrie. Si les Chinois[4] ont utilisé l'empreinte digitale aux fins de signature de documents il y a plus de mille ans, c'est Sir Francis Galton[5] qui au 19ème siècle a véritablement posé les fondements de la biométrie moderne en l'incluant très largement dans ses travaux sur l'hérédité et les différences individuelles. Il fit la démonstration que les empreintes digitales sont uniques et ne changent presque pas avec le vieillissement. La dactyloscopie ou l'identification par les empreintes digitales a finalement connu, entre la fin du 19ème siècle et le début du 20ème siècle, un succès grandissant jusqu'à être finalement adoptée par la plupart des forces de police de la planète.

Sans trop entrer dans le détail technique, il convient de retenir que les différents systèmes analysent les boucles, les tourbillons, les lignes et les verticilles des empreintes digitales. Les caractéristiques retenues s'appellent les minuties.

Les procédés optiques capturent à l'aide d'une caméra l'image d'une empreinte placée sur une vitre. Les technologies capacitives effectuent une analyse du champ électrique de l'empreinte digitale pour déterminer sa composition. Le stockage de la numérisation de cette empreinte se présente sous la forme d'une image, d'un code ou d'un numéro.

L'empreinte digitale pose une difficulté spécifique car elle est le seul élément biométrique omniprésent dans la sphère quotidienne. Il est en effet impossible de ne pas en laisser, y compris sur des objets à surface non lisse comme un vêtement. Elle constitue ainsi un moyen d'identification par traces presque aussi redoutable que l'ADN. Il convient donc de limiter l'utilisation de l'empreinte digitale comme procédé d'identification biométrique aux hypothèses les plus rares dans lesquelles les impératifs de sécurité exigent un niveau de protection particulièrement élevé.

L'alternative pourrait être de capturer les données sur un support portable telle une carte à puce. Ainsi stockées sur un support sécurisé et détenu exclusivement par la

[3] Op. cit. p. 7 ;
[4] Les chinois utilisaient déjà leurs empreintes de doigt pour sceller et signer des documents faits de bambou ;
[5] Ses travaux l'ont ensuite porté sur les chemins les plus rocailleux de la pensée eugéniste, à laquelle il aura beaucoup contribué ;

personne auxquelles elles appartiennent, l'entorse à la protection de la vie privée apparait atténuée.

Il a pu encore être avancé l'hypothèse d'un fichier central ne contenant que des données biométriques anonymes c'est à dire ne comportant aucun autre élément propre à permettre l'identification des personnes. La finalité d'une vérification ne nécessite pas plus que d'accorder ou refuser un accès ou donner droit à une classe de services sans qu'une identification ne soit pratiquée.

b) La forme de la main ou le contour de la main

L'utilisateur place sa main sur un gabarit éclairé par une lumière infrarouge et l'image qui en résulte est captée par une caméra digitale. Une centaine de caractéristiques sont extraites de l'image et sont converties en données stockées en mémoire. Il s'agit notamment de la longueur, la largeur, l'épaisseur de la main, la forme des articulations.

c) Le réseau veineux de la main ou du doigt

Les veines des mains sont un caractère spécifique à chaque individu. L'utilisateur place sa main dans une chambre, une caméra infrarouge lit alors les caractéristiques veineuses de la main, en extrait une image bidimensionnelle digitalisée qui est stockée pour comparaison ultérieure. Cette technique repose sur la reconnaissance de l'entrelacement des vaisseaux sanguins qui, contrairement à l'empreinte digitale, présente l'avantage d'être caché sous la peau. Il n'est donc pas possible en l'état des techniques actuelles de capturer et copier ces informations à l'insu de la personne.

d) La forme du visage

L'image du visage est captée par une caméra et le système en extrait les caractéristiques qui sont conservées dans une base de données. Par exemple, le procédé « *eigenface* » décompose l'image bidimensionnelle capturée en une série d'images teintées de nuances de gris. Il en résulte des zones grises et claires qui constituent les caractéristiques du visage de l'enrôlé. La méthode de « *feature analysis* » s'appuie plus particulièrement sur les déformations du visage, l'éclairage, les angles horizontaux et verticaux. La technique de l'« *automatic face* » calcule quant à elle les distances et ratios entre les yeux, le nez et la bouche.

e) Le balayage de la rétine

Les éléments qui permettent de distinguer deux rétines sont les veines qui les tapissent. La disposition de ces veines est stable et unique d'un individu à l'autre (d'un œil à l'autre). L'utilisateur place son œil à quelques centimètres d'un orifice de capture situé sur le lecteur de rétine. Il fixe alors un point lumineux qui effectue des rotations. Concomitamment un faisceau lumineux traverse l'œil jusqu'aux capillaires sanguins de la rétine pour localiser et capturer un certain nombre de points de référence.

f) La reconnaissance de l'iris

L'image de l'iris est lue par une machine contenant une caméra infrarouge ou ordinaire selon la distance qui la sépare l'individu. Le procédé capture quelques 250 caractéristiques de l'iris.

Pour distinguer les iris, on utilise les sillons de contraction, les cryptes, les anneaux, etc.

- La probabilité de trouver 2 iris suffisamment identiques est 1 sur 10 puissance 72 (selon une étude de Daugmann) ;

- Deux vrais jumeaux ont assez d'éléments distinctifs sur leur iris permettant de les distinguer l'un de l'autre.

g) La reconnaissance de la voix

A l'instar des éléments précédemment cités, la voix d'un individu est unique et elle peut être représentée graphiquement. La première étape du procédé consiste à créer une table de référence de la voix en demandant à l'individu de lire un texte. Des caractéristiques de la voix sont alors extraites : le débit, la force, la dynamique, la forme des ondes produites. Ces caractéristiques, qui forment une empreinte unique, sont traitées par un algorithme avant d'être finalement stockées. Il est important de capturer la voix dans des conditions optimales. En effet, bruit, réverbération et mauvais équipements jouent fortement sur la qualité des résultats enregistrés. Une fois cette étape préalable effectuée, la voix pourra être reconnu par la machine.

Traitement numérique de la voix

Pour pouvoir être traité numériquement, le signal sonore est numérisé sur 8 ou 16 bits à une fréquence d'échantillonnage qui varie entre 8 kHz et 48 kHz.

Présentation d'un système standard de reconnaissance de la voix :

1. Le signal acoustique est, dans un premier temps, analysé afin d'en extraire des paramètres. Ces paramètres résultent, entre autres, d'une analyse spectrale du signal (coefficients de prédiction linéaires ou bancs de filtres) ;
2. Les paramètres servent ensuite à l'élaboration éventuelle d'un modèle et sont introduits dans un « *classifieur* » (analyseur) qui permettra de déterminer l'identité du locuteur.

h) La reconnaissance de l'écriture

Il y a deux façons d'analyser une signature (écriture) : l'analyse statique et l'analyse dynamique :

- **Analyse statique** : elle utilise la géométrie de la signature. L'avantage de cette méthode est qu'elle est bien adaptée pour authentifier des documents manuscrits. La vérification automatisée des chèques dans les banques est une des applications intéressantes, Un scanner spécial rend cette opération plus rapide et plus sûre qu'avec un opérateur ;
- **Analyse dynamique** : elle utilise les paramètres statiques ainsi que l'accélération, la vitesse et les profils de trajectoire de la signature (voir illustration ci-dessus). L'avantage indéniable est l'impossibilité pour un imposteur de reproduire une signature avec les mêmes informations dynamiques que l'original. Cependant, elle nécessite une capture directe de la signature sur une tablette tactile.

i) La dynamique de frappe au clavier

Il s'agit d'un dispositif logiciel qui calcule le temps où un doigt effectue une pression sur une touche et le temps où un doigt est en l'air entre les frappes. Les mesures sont effectuées mille fois par seconde. La séquence de frappe est prédéterminée par un mot de passe qui est effectué plusieurs fois par l'utilisateur aux fins de constituer un gabarit de référence.

II) La loi 1.165 appliquée à la biométrie

A. Le régime applicable : l'autorisation préalable

L'article 11-1 de la loi susmentionnée dispose que :

« *Par dérogation aux dispositions de l'article précédent, peuvent être mis en œuvre, par les responsables de traitements autres que les autorités judiciaires et administratives, les traitements automatisés d'informations nominatives :*

- *portant sur des soupçons d'activités illicites, des infractions, des mesures de sûreté ;*
- *comportant des données biométriques nécessaires au contrôle de l'identité des personnes ;*
- *mis en œuvre à des fins de surveillance.*

Lesdits traitements ne peuvent toutefois être mis en œuvre qu'avec l'autorisation préalable de la commission de contrôle des informations nominatives dès lors qu'ils sont nécessaires à la poursuite d'un objectif légitime essentiel et que les droits et libertés mentionnées à l'article premier des personnes concernées sont respectés ».

Il résulte donc de la rédaction de l'article 11-1 que sont concernés tous responsables de traitements autres que les autorités judiciaires et administratives. Il s'agit donc de l'ensemble des responsables de traitements des personnes physiques ou morales de droit privé ou public, qui ne répondent pas à la définition d'autorité judiciaire ou d'autorité administrative.

Les traitements « *comportant des données biométriques nécessaires au contrôle de l'identité des personnes* » ou « *mis en œuvre à des fins de surveillance* » sont placés expressément sous le régime de l'autorisation préalable telle que prévue par les dispositions de la loi n° 1.165 du 23 décembre 1993 modifiée. Il convient de noter que ladite loi a, dans sa rédaction actuelle, entouré le recours à la biométrie très strictement.

Le tiret second de l'énumération susmentionnée énonce que les données biométriques doivent être nécessaires au contrôle de l'identité des personnes. Le terme de « *nécessité* » est en soi sujet à réflexion : Cette nécessité doit-elle être entendue dans son acception « *impérieuse* », ou laisse-t-elle place à un certain degré d'appréciation ?

Le second alinéa offre un éclairage utile à la notion de « *nécessité* » : Les traitements doivent être nécessaires à la poursuite d'un objectif légitime essentiel.

Cette disposition se fait l'écho de l'article 10-1 de la loi 1.165 susvisée, qui énonce expressément que les informations nominatives doivent être collectées pour une finalité déterminée, explicite et légitime et ne pas être traitées ultérieurement de manière incompatible avec cette finalité. Ledit article ne manque pas encore de préciser que les informations nominatives doivent être adéquates, pertinentes et non excessives au regard de la finalité pour laquelle elles sont collectées.

Il s'en infère que les caractères « *légitime* » et « *essentiel* » évoqués à l'article 11-1 se rapportent directement au caractère non excessif. Le caractère excessif ou non peut être apprécié suivant le crible d'une analyse quantitative et qualitative. La collecte d'une donnée biométrique permettant une intrusion trop importante dans la vie privée de l'individu est à elle seule excessive. Il faut alors prévoir en amont que le « *gabarit* » soit constitué de façon à ne

relever que ce qui est nécessaire à la finalité du système. Par exemple, si l'analyse de l'iris est susceptible de faire état d'une maladie, il est impératif que le « *gabarit* » ne contienne que des informations relatives à sa géométrie. Seule la finalité du traitement permettra véritablement de se prononcer sur le caractère excessif ou non du traitement et des données utilisées.

La question de la conservation des données biométriques se décompose en trois points. Premièrement, les données biométriques enrôlées sont conservées sur un support de stockage. Ces données ne devront pas être conservées pour une durée supérieure à la finalité pour laquelle elles sont enregistrées. Deuxièmement, les données obtenues lors de la collecte secondaire ne sont d'aucune utilité après leur comparaison avec les données enrôlées. Ces données devraient le plus souvent être effacées immédiatement puisqu'elles ne tendent qu'à une finalité immédiate de comparaison avec les données enrôlées. Troisièmement, la conservation des données associées pose plus de difficulté compte tenu des dérives potentielles qui s'y rapportent.

Dans le cadre de zones nécessitant un degré de sécurité particulièrement élevé, il peut être légitime de déterminer qui s'est rendu dans une zone déterminée et pour combien de temps. Dans ce cas, les données secondaires ne visent pas à s'assurer du bon fonctionnement du système mais se rapportent directement au processus d'identification. Dans tous les cas, la conservation des données associées à des fins incompatibles avec la finalité du système doit être interdite. Pour les données associées compatibles avec la finalité du système, elles devront être justifiée au regard de celle-ci.

En outre, s'agissant de données biométriques, il convient de prévoir des mesures de sécurité spécifiques conformément aux article 17 et 17-1 de la loi n° 1.165 du 23 décembre 1993 pour « *protéger les informations nominatives contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions d'informations dans un réseau, ainsi que contre toute autre forme de traitement illicite* ». Les mesures mises en œuvre devront présenter un niveau de sécurité adéquat au regard des risques présentés par le traitement et de la nature des données à protéger.

Des normes ou standards de qualité des logiciels et des matériels devraient être envisagés. L'article 17-1 énonce que « *lorsque le traitement est mis en œuvre en application des articles 11 et 11-1 le responsable du traitement prend, en outre, des mesures techniques et d'organisation particulières destinées à garantir la protection des données. La liste des mesures susceptibles d'être prises à cette fin est fixée par ordonnance souveraine* ».

L'ensemble des procédés biométriques devraient utiliser des algorithmes d'un niveau de qualité à définir pour extraire le gabarit de l'image biométrique et comparer les données enrôlées avec celles soumises par la suite. Par ailleurs et en droite ligne avec le « *Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques* » de 2005 l'utilisation du cryptage semble nécessaire pendant le processus d'enrôlement « *pour éviter que des personnes non autorisées puissent accéder à des données brutes et les utiliser pour usurper l'identité de l'utilisateur légitime* ». Le même rapport préconise un cryptage sophistiqué des données biométriques pendant le processus d'enrôlement, pour le stockage et la transmission sur des lignes de télécommunication pour renforcer la sécurité et rendre plus difficile l'usage non autorisé des données biométriques. L'interception sauvage d'un signal crypté sans la clé de décryptage ne permettrait pas la reconstruction du signal de réponse du système biométrique.

B. Les garanties de la personne soumise à un traitement biométrique

- **<u>Le droit d'être informé</u>**

Les personnes concernées devraient être valablement informée conformément aux dispositions de l'article 14 de la loi n° 1.165 modifiée.

- **Le droit d'accès**

L'article 15 de la loi n° 1.165 modifiée prévoit que « *toute personne justifiant de son identité peut obtenir auprès du responsable du traitement ou de son représentant :*

1°) des renseignements portant au moins sur la finalité du traitement, les catégories d'informations sur lesquelles il porte et les destinataires ou catégories de destinataires auxquels les informations sont communiquées ;

2°) confirmation que des informations la concernant sont, ou non, traitées ;

3°) communication de ces informations sous une forme écrite, non codée et conforme au contenu des enregistrements ; les informations à caractère médical sont communiquées à la personne concernée, ou au médecin qu'elle aura désigné à cet effet. En cas d'avis contraire médicalement justifié, les informations ne peuvent être communiquées qu'audit médecin. Les conditions d'application du présent chiffre sont définies par ordonnance souveraine ;

4°) des informations sur les raisonnements automatisés ayant abouti à la décision visée à l'article 14-1.

Il doit être procédé à la communication dans le mois suivant la réception de la demande. Toutefois, le président de la commission de contrôle des informations nominatives peut, après avis favorable de celle-ci, accorder des délais de réponse ou dispenser de l'obligation de répondre à des demandes abusives par leur nombre, leur caractère répétitif ou systématique, la personne concernée dûment avisée ».

Ainsi, toute personne peut accéder aux données biométriques qui la concerne. Ce droit doit aussi s'appliquer aux « *données associées* » qui révèlent des informations complémentaires, comme par exemple l'heure et le lieu de passage de l'individu. Plus généralement, toute personne doit pouvoir accéder à toute information se rapportant à son identité dans le cadre d'un traitement de données biométriques.

- **Le droit d'opposition de l'article 13**

Une difficulté peut surgir s'agissant des organismes visés à l'article 7 de la loi n° 1.165, agissant dans le cadre exclusif de leur mission d'intérêt général : Les personnes ne pourraient pas s'opposer à ce que l'information biométrique les concernant fasse l'objet d'un traitement.

A l'égard de ces traitements, il convient d'être particulièrement strict sur le champ d'application de cet article et vigilant quant aux mesures de sécurité mises en place dans le cadre de tels traitements.

- **Le droit de rectification, de complément et d'effacement**

L'article 16 de la même loi prévoit un droit de rectification et d'effacement des informations inexactes:

« *La personne intéressée peut exiger que soient rectifiées, complétées, clarifiées, mises à jour ou supprimées les informations la concernant lorsqu'elles se sont révélées inexactes, incomplètes, équivoques, périmées ou si leur collecte, leur enregistrement, leur*

communication ou leur conservation est prohibé. Sur sa demande, copie de l'enregistrement de l'information modifiée lui est délivrée sans frais. S'il y a eu communication à des destinataires, l'information modifiée ou sa suppression doit leur être notifiée, sauf dispense accordée par le président de la commission de contrôle des informations nominatives ».

La question de l'inexactitude se rapporte au procédé biométrique même qui de part sa nature est probabiliste. Pendant la phase d'enrôlement, l'algorithme qui extrait le « *gabarit* » de la caractéristique biométrique peut être plus ou moins étendu selon la finalité du système. Un algorithme moins étendu génère un gabarit moins spécifique qui est donc sujet à plus de « *faux rejets* » et plus de « *fausses acceptations* ». L'étendue de l'algorithme doit donc être guidée par la finalité du traitement.

Les droits de rectification, de complément, de clarification, de mise à jour et de suppression se justifient donc pleinement à la lumière des erreurs possibles du système et auxquelles pourraient par ailleurs être adjointes des « *données associés* » inexactes. Par exemple, il est possible qu'un individu autorisé et accepté par le système se voit adjoindre une erreur d'heure ou de date qui serait liée non à la partie du système consacrée à l'analyse biométrique mais à celle qui définit l'heure et la date du passage.

Les causes de l'absence de reconnaissance de l'individu par le système biométrique peuvent être variées et complexes. Le choix du recours au procédé biométrique étant de la responsabilité du responsable de traitement, il conviendra que la situation de la personne soumise à un « faux rejet » puisse être corrigée immédiatement ou dans un très bref délai, notamment par la mise en place d'une solution alternative ou supplétive par exemple pour permettre l'accès à la personne légitime non autorisée.

La question de la solution alternative ou supplétive ne se pose d'ailleurs pas uniquement dans cette hypothèse mais également pour les personnes présentant des caractéristiques physiques incompatibles avec le fonctionnement du procédé biométrique (un handicap par exemple).

- **L'interopérabilité**

Sur la question de l'interopérabilité, l'article 16 in fine prévoit que s'« *il y a eu communication à des destinataires, l'information modifiée ou sa suppression doit leur être notifiée, sauf dispense accordée par le président de la commission de contrôle des informations nominatives* ».

A l'heure du partage et de la mise en commun tant des ressources que des supports qui se dématérialisent irrémédiablement, il semble particulièrement dangereux d'autoriser des procédures standardisées pour permettre à différents systèmes d'interagir. L'interopérabilité de systèmes dotés d'une fonction de compatibilité permettrait de reconnaître les personnes en fonction de leur données biométriques indépendamment de toute faute du responsable de traitement. La question de l'interopérabilité et du transfert des données biométrique devra appeler à une particulière vigilance.

L'article 16 in fine ne sécurise pas totalement la situation de l'individu soumis à un traitement de données biométriques. Si l'information inexacte s'est propagée, le responsable du traitement doit notifier la modification de l'information ou sa suppression aux destinataires qui ont eu communication de cette information (sauf dispense). Il s'en infère que le responsable de traitement n'a pas d'autre formalité à accomplir autre que ladite notification, ce qui dans le cadre d'un traitement de données biométriques soulève la question de l'effectivité du recours de la personne au regard de la complexité du procédé. La solution se trouve probablement en amont dans l'octroi éventuel d'un droit de transfert des données biométriques. Les dimensions géographiques de la Principauté de Monaco et sa population

semblent être des éléments importants à considérer dans la question de l'usage de la biométrie en Principauté de Monaco.

CONCLUSIONS : la position de la Commission

Au regard de ce qui précède et eu égard à la nouveauté de tels procédés, la Commission souhaite conserver une certaine prudence à l'égard de la biométrie et prendre un certain recul sur une matière en pleine évolution. Elle décide cependant de permettre le recours à certains types de biométries pour ne pas pénaliser les organismes et entreprises désireux de bénéficier de ces nouvelles technologies.

Ainsi, le recours aux biométries dites « *non traçantes* » a, à l'instar des autres autorités de contrôle, la préférence de la Commission. Par ailleurs, elle est vigilante sur la méthode de stockage employée pour la conservation de l'information biométrique.

En l'état de ses réflexions, la Commission autorisera, dans le strict cadre des délibérations portant recommandations :

A) Les dispositifs portant sur la reconnaissance du contour de la main, avec stockage de la donnée biométrique sur un support individuel ou dans une base de données et ayant pour finalité le contrôle de l'accès et/ou la gestion des horaires sur le lieu de travail, mis en œuvre par les personnes physiques ou morales de droit privé ;

B) Les dispositifs portant sur la reconnaissance du réseau veineux du doigt de la main et de la main, avec stockage de la donnée biométrique sur un support individuel ou dans le terminal de lecture-comparaison, à l'exclusion de tout autre stockage dans une base de données, ayant pour finalité le contrôle de l'accès aux locaux sur le lieu de travail, mis en œuvre par les personnes physiques ou morales de droit privé ;

C) Les dispositifs ayant pour finalité le « *Contrôle d'accès par reconnaissance de l'empreinte digitale* », limités rigoureusement à des situations spécifiques.

Ainsi, il convient de noter que le recours à la méthode de la reconnaissance du contour de la main est plus ouvert que celle de la reconnaissance du réseau veineux du doigt. Cela est inhérent à la nature même de la donnée collectée. La méthode de la reconnaissance du contour de la main est peu discriminante et elle est sensible aux modifications ou altérations naturelles de la main (accident, vieillissement, arthrose…), ce qui justifie par ailleurs le stockage de la donnée dans une base de données (un serveur par exemple). Cela pourra également justifier qu'il soit procédé à la mise à jour des terminaux de lecture-comparaison au moyen de ladite base de données. En effet, l'information primitive se limite à la morphologie de la main, la largeur de la paume de la main, la longueur et l'épaisseur des doigts, notamment. Elle pourra d'ailleurs être associée un numéro de badge en complément d'information pour ce système aux fins d'endiguer les risques de faux rejets.

A contrario, la donnée issue du réseau veineux du doigt est une technique très fiable qui ne nécessite pas de contact sur le terminal et en ce qu'elle constitue une information beaucoup plus spécifique, le recours à cette méthode justifie un encadrement plus strict.

Enfin, la méthode de la reconnaissance de l'empreinte digitale pose des difficultés spécifiques en ce qu'elle constitue une biométrie particulièrement traçante. La Commission considère que le stockage d'une telle information dans une base de données constitue un risque trop important en considération des spécificités de la Principauté de Monaco.

Les demandes d'autorisations s'appuyant sur l'empreinte digitale avec stockage sur une base de données centralisée seront examinées par la Commission au cas par cas et au regard d'un risque d'une particulière gravité nécessitant le recours à une telle technique.

Toutefois et pour ne pas léser les organismes et entreprises tenus de recourir à la méthode de la reconnaissance par empreinte digitale, notamment au regard d'une obligation légale, la Commission autorise, dans certaines hypothèses, le recours aux dispositifs portant sur la reconnaissance de l'empreinte digitale, avec stockage de la donnée biométrique sur un support individuel et à l'exclusion de toute autre forme de stockage, ayant pour finalité le contrôle d'accès à des zones limitativement identifiées sur le lieu de travail, mis en œuvre par les personnes physiques ou morales de droit privé.

Enfin, eu égard aux spécificités attachées aux techniques biométriques sus décrites, il conviendrait d'entourer le recours à la biométrie des garanties qui suivent, inspirées du rapport d'étape de la Convention 108 susvisé.

RECOMMANDATIONS GENERALES, ADAPTEES DU RAPPORT D'ETAPE DE LA CONVENTION 108

1- Le recours à la biométrie doit faire l'objet, par le responsable de traitement, d'une évaluation préalable des avantages et inconvénients au regard de l'activité concernée, afin d'anticiper d'éventuelles atteintes à la vie privée. Dans cette hypothèse, il conviendra de justifier de telles atteintes en démontrant la nécessité de recourir à une telle technique au regard de la finalité recherchée. En effet, ces atteintes ne doivent en aucun cas être disproportionnées ou excessives au regard du but recherché.

2- La biométrie ne doit pas être envisagée pour une finalité de confort, mais être justifiée par des impératifs de nécessité.

3- Le recours à la biométrie doit, conformément à l'article 11-1 de la loi n° 1.165, modifiée, être soumis à l'autorisation préalable de la CCIN, dès qu'il aura été établi par le responsable de traitement que le recours à cette technique est « *nécessaire à la poursuite d'un objectif légitime essentiel et que les droits et libertés mentionnés à l'article premier des personnes concernées sont respectés* ».

4- Les données biométriques objets du traitement ne doivent être utilisées à des fins différentes ou incompatibles avec les finalités initialement présentées à la CCIN.

5- conformément à l'article 10-1 de la loi n° 1.165, modifiée, les données biométriques collectées doivent toujours être adéquates, pertinentes et non excessives au regard de la finalité du traitement. La méthode de traitement envisagée ne doit jamais recueillir plus d'informations que nécessaire à la poursuite du but envisagé.

6- Le choix entre le stockage sur un support individuel ou sur une base de données centralisée doit toujours être justifié et conforme à l'impératif de sécurité. D'une manière générale, le choix d'une méthode de stockage sur support individuel sécurisé de stockage (type carte à puce personnelle) doit être préféré à celui d'une méthode requérant le stockage dans une base de données centralisée.

7- Les matériels et les logiciels utilisés aux fins de mise en place du procédé biométrique envisagé, doivent respecter un degré de fiabilité suffisant au regard de l'évolution des techniques.

8- La personne dont les données biométriques sont collectées doit, en toutes hypothèses, être informée de la finalité du traitement, de l'identité du responsable de traitement, de la nature des données traitées et des catégories de personnes auxquelles les données seront communiquées, le cas échéant.

9- La personne concernée par le traitement dispose d'un droit d'accès, de rectification, et d'effacement de ses données.

10- Le responsable de traitement doit s'assurer du respect effectif des droits de la personne concernée, en prévoyant toutes les mesures techniques nécessaires aux fins de prévenir, notamment, la destruction, le piratage, la perte, l'accès illicite, la modification illicite et la communication non autorisée des données objets du traitement biométrique.

11- Dans l'hypothèse où une personne serait rejetée par le système biométrique, le responsable du traitement doit, sur simple demande, apporter les corrections nécessaires et une solution supplétive immédiate.