Examen de la mise en œuvre par divers organismes de traitements de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux

rapport de *Hubert Bouchet,* membre de la CNIL (1)

PLAN

Sont aujourd'hui présentés à la Commission huit traitements de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux. Tous ces dispositifs impliquent un enregistrement des empreintes digitales des employés au sein d'une base de données située sur un serveur central ou directement au niveau du lecteur biométrique.

Compte tenu de ces éléments, il y a lieu pour la Commission de faire application des dispositions de l'article 25-8° de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

Dans ce contexte, votre rapporteur propose d'effectuer une brève présentation des fonctionnalités et modalités de mise en œuvre des dispositifs projetés (I), pour ensuite procéder à leur analyse au regard de la loi du 6 janvier 1978 modifiée en août 2004 et des décisions déjà adoptées par la Commission en vue de déterminer s'ils sont proportionnés ou non par rapport aux finalités poursuivies (II).

I. Présentation des dispositifs soumis à la Commission

A. Le groupe Rothschild

Le 23 septembre 2005, quatre sociétés appartenant au groupe Rothschild (2) ont adressé à la Commission des déclarations normales relatives à la mise en œuvre de dispositifs strictement identiques reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de *« contrôler l'accès aux salles informatiques et téléphoniques de la société qui renferment des données hautement sensibles ».*

Dans le cadre d'un courrier de demande de compléments daté du 27 octobre 2005, les services de la Commission ont informé les différentes sociétés concernées que ce type de traitement relevait du régime d'autorisation.

Les dispositifs projetés reposent sur plusieurs boîtiers de marque Sagem répartis à l'entrée des salles informatiques et téléphoniques dont l'accès est limité à certains employés habilités. Chaque appareil fonctionne de manière isolée et n'est relié à aucun réseau. Il est en outre précisé que toute tentative de récupération des données

(1) Avec le concours de Mathias Moulin, attaché à la direction des affaires juridiques. NDLR : deux délibérations sont reproduites en annexe au présent rapport ; les autres délibérations (2006-154, 2006-155 et 2006-156) sont disponibles sur www.legifrance.fr rubrique *Autorités administratives indépendantes.*

(2) Il s'agit de :
- la société Rothschild & Cie Gestion (gestion de portefeuilles) ;
- la société Rothschild & Cie (organisme de placement en valeurs mobilières) ;
- la société Rothschild & Cie banque ;
- la société Rothschild Gestion (gestion de portefeuilles).

engendre une destruction immédiate des informations stockées à savoir, un numéro d'identification auquel est associé le gabarit (3) de l'empreinte digitale des employés concernés. Il est également indiqué que le matériel utilisé est en mesure de détecter les tentatives de fraude reposant sur un faux doigt ou « doigt mort ».

Lors du contrôle d'accès, l'employé appose son doigt sur le lecteur biométrique du boîtier, une comparaison s'effectue alors entre cette empreinte digitale et le gabarit enregistré dans la base de données du lecteur. Aucun historique des passages n'est réalisé à cette occasion.

Il convient de préciser que les services généraux conserveront une liste permettant de faire le lien entre chaque numéro d'identification et l'identité des employés concernés. Par ailleurs, la direction des ressources humaines, le service juridique et fiscal et le service de la sécurité détiendront une liste des personnes dont le gabarit figure dans un des lecteurs. Il est également précisé que le *« service sécurité conservera la liste des personnes enregistrées dans chaque appareil biométrique ainsi que le gabarit de chacun des utilisateurs dans le lecteur des empreintes digitales »*.

Une information et une consultation du comité d'entreprise ont été effectuées conformément aux dispositions de l'article L. 432-2 du Code du travail. Ce dernier a rendu à l'unanimité le 8 décembre 2005 un avis favorable à l'introduction du système envisagé.

Par ailleurs, les employés concernés se verront remettre un formulaire intitulé « autorisation de prélèvement des empreintes digitales » dans le cadre duquel ils autorisent leur employeur à procéder à l'enregistrement de leurs empreintes digitales (index droit et gauche ainsi que le pouce) aux fins de pouvoir accéder à une salle identifiée. Ce document ne fait aucune mention des destinataires des données, ni de l'existence d'un droit d'accès, de rectification ou d'opposition.

En revanche, les compléments d'information adressés par les sociétés du groupe Rothschild (4) précisent que *« les collaborateurs n'ont aucune obligation de faire enregistrer leurs empreintes digitales, quand bien même l'accès à ces salles pourrait présenter pour l'exercice de leur travail un intérêt évident. L'enregistrement des empreintes par les collaborateurs résulte de leur libre choix. Ils sont assurés qu'il ne sera pris à leur encontre aucune sanction, de quelque nature qu'elle soit. »*

Enfin, lors du départ d'un employé, son empreinte sera immédiatement supprimée du lecteur par l'un des responsables du service sécurité. Il est également envisagé de détailler au sein d'une procédure les modalités pratiques de sortie des employés et d'inclure à cette occasion un article relatif à la suppression des données biométriques.

B. La Mesta Chimie Fine SA

Le 16 mars 2006, la société La Mesta Chimie Fine SAS a obtenu de la Commission l'autorisation (5) de mettre en œuvre un dispositif de reconnaissance des empreintes digitales avec enregistrement sur un support individuel aux fins de contrôler l'accès à un site relevant de la réglementation sur les installations classées pour la protection de l'environnement (ICPE) de type « SEVESO seuil bas ». Cependant, au terme d'un mois d'utilisation, le dispositif s'est révélé inadapté à la finalité qui lui est assignée et aux besoins de la société La Mesta Chimie Fine SA. En conséquence, cette dernière a adressé à la Commission une demande d'autorisation modificative (6) afin de pouvoir enregistrer les empreintes digitales dans une base de données et non plus au sein d'un support individuel.

Ainsi, le nouveau dispositif présenté devrait reposer sur plusieurs boîtiers répartis aux différents points d'accès au site et au local de maintenance. Les gabarits des empreintes digitales des personnes habilitées à accéder au site et au local de maintenance seront enregistrés dans ces boîtiers. Ces derniers seront reliés à un serveur au niveau duquel seront enregistrées les identités des employés (nom, prénom).

Lors du contrôle d'accès, l'employé appose son doigt sur le lecteur biométrique du boîtier, une comparaison s'effectue alors entre cette empreinte digitale et le gabarit enregistré dans la base de données du lecteur. Les données relatives à l'historique des passages seront conservées pendant un mois. La durée de conservation relative à l'identité de l'employé et au gabarit de l'empreinte digitale, sera égale au temps pendant lequel la personne concernée travaille pour la société Mesta Chimie Fine.

Une information et une consultation du comité d'entreprise ont été effectuées conformément aux dispositions de l'article L. 432-2 du Code du travail. L'information individuelle des employés est effectuée au moment de l'enrôlement. Les employés peuvent accéder en ligne à leur dossier comportant l'historique de leurs passages après saisie d'un mot de passe et d'un nom d'utilisateur.

Enfin, les mesures prises en vue de garantir la sécurité des données, apparaissent conformes à l'état de l'art et aux exigences de la Commission.

S'agissant du contrôle d'accès logique au système, les éléments d'informations figurant dans les dossiers

(3) Clé biométrique correspondant à une chaîne de caractères.

(4) Courrier reçu par la CNIL le 3 janvier 2006.

(5) Délibération n° 2006-071.

(6) Courrier daté du 26 avril 2006.

apparaissent satisfaisants notamment, concernant l'administration des mots de passe et la politique de gestion des accès dans la mesure où, seuls le responsable Hygiène et sécurité et le chef de service administratif disposent de l'habilitation pour accéder aux données.

Enfin, il convient de préciser d'une part, que l'accès à l'application et aux fichiers contenant les données à caractère personnel fera l'objet d'une journalisation et, d'autre part, que le dispositif repose sur un réseau privé permettant de prévenir tout risque d'intrusion extérieure.

II. Appréciation des dispositifs au regard de la loi du 6 janvier 1978 modifiée en août 2004

A. Rappel de la doctrine de la CNIL de la CNIL sur l'utilisation de l'empreinte digitale à des fins de contrôle de l'accès aux locaux

La CNIL n'admet la mise en œuvre de bases de données d'empreintes digitales que dans la mesure où un impératif particulier de sécurité le justifie. Depuis le 10 juin 1997, date à laquelle la Commission a pour la première fois délivré un avis favorable à la Banque de France concernant un dispositif reposant sur le stockage centralisé des empreintes digitales et ayant pour finalité de contrôler l'accès à des zones hautement sécurisées (délibération n° 97-044), elle n'a autorisé la mise en œuvre que d'une douzaine de dispositifs similaires et pour lesquels il existait à chaque fois un impératif particulier de sécurité (7).

Ce fut, par exemple, le cas de la Cité académique de Lille qui a obtenu un avis favorable de la CNIL le 21 mars 2000 (8) s'agissant d'un dispositif de contrôle d'accès à certains locaux en vue de garantir la confidentialité des sujets d'examens et de concours. On citera également la société Aéroport de Paris pour le contrôle de l'accès aux "zones réservées sécurité", l'Imprimerie nationale (9) ou plus récemment encore la société Sagem Défense Sécurité qui a obtenu l'autorisation de la Commission concernant un dispositif devant permettre de contrôler l'accès au site de Montluçon et notamment à des zones réservées "secret défense" au sein de cet établissement (10).

A contrario, en l'absence d'un impératif particulier de sécurité, la Commission a jusqu'à présent toujours estimé que si une base de données de gabarits devait être constituée, le choix d'un élément biométrique « ne laissant pas de trace », tel que le contour de la main ou la rétine, devrait être préféré à la constitution de fichiers d'empreintes digitales.

A ce titre, la Commission a émis un avis défavorable le 16 décembre 2003 sur un projet de création d'un dispositif de reconnaissance des empreintes digitales pour contrôler l'accès des abonnés à un "roller-parc". Elle a en effet estimé que « *l'objectif invoqué par la mairie de se doter d'un dispositif évitant la manipulation de cartes pour gérer les accès ne justifie pas la conservation dans une base de données des empreintes digitales des personnes fréquentant le "roller-parc"* » (délibération 03-065).

Auparavant, elle avait fait de même s'agissant d'un système de contrôle de l'accès à une cantine scolaire présenté par le Lycée Jean Rostand de Nice (délibération n° 00-015 du 21 mars 2000).

Plus récemment encore, le 12 janvier dernier, la Commission a refusé la mise en œuvre de quatre dispositifs reposant sur la reconnaissance des empreintes digitales avec un stockage centralisé. Il s'agissait là aussi de trois dispositifs de contrôle d'accès aux locaux :

– la société Air Promotion Group proposant des services de centres d'appels spécialisés, d'intégration des horaires et tarifs dans les systèmes de réservation disponibles en agences de voyages, d'interfaçage des systèmes de billetterie avec les autres compagnies aériennes (délibération n° 2006-002) ;

– le cabinet de conseil en propriété industrielle Breese – Derambure – Majerowicz (délibération n° 2006-003) ;

– la Société du Marché d'Intérêt National d'Avignon (SMINA) Société d'économie mixte pour la construction et l'exploitation du Marché Gare (délibération n° 2006-005).

La Commission avait considéré à cette occasion que l'objectif invoqué, s'il était légitime, n'était associé à aucun impératif de sécurité particulier et ne justifiait pas dès lors la conservation dans une base de données des empreintes digitales des employés habilités à accéder aux locaux.

Par ailleurs, la Commission a également souligné le caractère exceptionnel des bases de données d'empreintes digitales au travers de l'adoption le 27 avril dernier d'une autorisation unique relative aux dispositifs de contrôle d'accès reposant sur l'empreinte digitale avec enregistrement sur support individuel (11).

(7) Cf. liste en annexe 7.

(8) Délibération n° 00-015 - Avis favorable n° 04-017 du 8 avril 2004.

(9) Délibération n° 2005-113 du 7 juin 2005, concernant le contrôle d'accès aux locaux où sont produits les documents d'identité tels que les passeports et les cartes grises.

(10) Délibération n° 2006-070 du 16 mars 2006.

(11) Autorisation unique n° 8 - Délibération n° 2006-102. NDLR : un commentaire des deux autorisations uniques de la CNIL a été réalisé au Dr. Ouv. 2007 p. 31.

Ainsi, il convient à présent de confronter les cas aujourd'hui soumis à la Commission aux exigences et critères qu'elle a pu dégager lors de l'examen des dossiers précités, afin de déterminer s'ils sont ou non proportionnés au regard de la finalité qui leur est assignée.

B. Proportionnalité des dispositifs au regard de la finalité poursuivie

A diverses occasions, les services de la Commission ont attiré l'attention des sociétés précitées sur le fait que le recours à un dispositif reposant sur la reconnaissance des empreintes digitales, dès lors que ces dernières sont enregistrées dans une base de données centralisée ou sur le lecteur, ne saurait être justifié qu'en présence d'un impératif particulier de sécurité.

En conséquence, les sociétés concernées ont adressé à la CNIL des compléments d'information tendant à démontrer que le dispositif était justifié par un impératif particulier de sécurité.

1. Le groupe Rothschild

Pour justifier de la nécessité d'avoir recours à un dispositif reposant sur la reconnaissance des empreintes digitales avec enregistrement dans une base de données, les sociétés du groupe Rothschild invoquent tant les contraintes existantes dans le secteur bancaire (b) que des arguments techniques propres au dispositif utilisé (a). Au préalable, il convient de relever qu'une des sociétés du groupe Rothschild, la Compagnie Financière Edmond de Rothschild, avait déjà adressé à la Commission un dossier de formalité préalable relatif à un dispositif similaire le 22 novembre 2002 (12).

a) Examen des arguments techniques

En premier lieu, les sociétés du groupe Rothschild indiquent que *« l'appareil Sagem Morphoaccess MA 200 n'effectue aucune imagerie d'empreinte digitale (ni photo, ni dessin des empreintes digitales). Il s'agit de données numérisées qui ne peuvent en aucune manière servir à la reconstitution d'une empreinte digitale ».*

Sur ce point, le service de l'expertise informatique de la Commission qui a eu à rendre un avis (13) sur les dispositifs présentés précise que *« […] dans un certain sens, le gabarit d'une empreinte est encore plus identifiant que l'empreinte d'origine dont il est issu puisqu'il est construit à partir des seules caractéristiques "utiles" figurant dans celle-ci. Toute argumentation tendant à nier (ou à minimiser) le caractère "biométrique" d'un procédé dès lors que seuls les gabarits sont traités (ou stockés) n'a donc aucun sens, cela pour deux motifs principaux :*

– le gabarit est calculé à partir d'un échantillon biométrique qu'il a bien fallu préalablement collecter,

– le gabarit n'est qu'une simple représentation numérique des caractéristiques utiles figurant dans l'échantillon collecté. »

Par ailleurs, les sociétés du groupe Rothschild affirment que « *les informations stockées dans l'appareil sont inutilisables et non récupérables [...] il est impossible de reproduire une empreinte à partir d'un référentiel, puisque celles-ci n'existent pas à l'état d'image, et de l'utiliser à d'autres fins*. »

En réponse, le service de l'expertise indique que « *l'exploitation d'un gabarit, dès lors que sont connues les règles qui permettent de le construire* (14)*, ne pose aucun problème pour un informaticien. Privilégier l'image numérisée comme plus "authentique" que le gabarit n'a donc aucun sens : sur le plan informatique* (15)*, l'un et l'autre représentent tout autant l'échantillon analogique d'origine, mais pour des finalités différentes (la première destinée principalement à l'affichage ou à l'impression sur papier, l'autre pour un contrôle biométrique […])* ». De même, il précise que « *toute empreinte digitale collectée sur un lieu peut être soumise au contrôle du boîtier Morphoaccess afin qu'il réponde à la question : oui ou non cette empreinte figure-t-elle dans la liste des empreintes stockées dans la mémoire du boîtier ? Que le gabarit soit crypté ou non ne change rien à cette capacité du boîtier de pouvoir répondre à une telle question* ».

Il apparaît ainsi que les arguments techniques avancés par les sociétés du groupe Rothschild ne permettent pas en tant que tels d'autoriser la mise en œuvre des traitements projetés. Dès lors, il appartient à la Commission de décider si les contraintes sécuritaires inhérentes au secteur bancaire suffisent à elles seules à justifier le recours à des dispositifs reposant sur la reconnaissance des empreintes digitales avec un enregistrement dans une base de données.

b) Appréciation au regard de l'activité exercée

S'agissant de la nécessité d'avoir recours à une telle technologie, les sociétés du groupe Rothschild soulignent que leur activité dépend dans une large mesure du bon fonctionnement des serveurs informatiques et des répartiteurs téléphoniques dont il s'agit d'encadrer les conditions d'accès physique.

(12) Déclaration ordinaire n° 828963.

(13) Cf. annexe 1, non reproduite.

(14) A cet égard, on relèvera que l'algorithme permettant de générer un gabarit relève du secret professionnel que les industriels sont par exemple tenus de communiquer aux autorités judiciaires dans les conditions prévues par le Code de procédure pénale.

(15) La vision humaine reconnaît évidemment mieux la parenté entre une image numérisée affichée sur un écran et l'image d'origine qu'avec le gabarit, mais pour l'informatique, l'une et l'autre, image numérisée et gabarit, ne forment qu'une succession de chiffres 0 et 1 qu'il lui faut interpréter.

Les serveurs informatiques enregistrent tous les fichiers créés par l'ensemble des employés, il est ainsi indiqué *« que tout acte de malveillance ou même accidentel provoquant un dysfonctionnement ou une panne de ces serveurs entraînerait une dégradation ou un arrêt immédiat de tous les systèmes informatiques et téléphoniques des collaborateurs de la banque, ce qui gênerait fortement voire empêcherait toute poursuite de l'activité. »*

Si l'argument énoncé ci-dessus doit être pris en considération, il ne saurait en revanche justifier à lui seul la mise en œuvre du dispositif présenté et ce, dans la mesure où d'une manière générale les systèmes d'information revêtent une importance stratégique pour l'exercice de la plupart des activités industrielles ou de service. Le cas des sociétés du groupe Rothschild ne constitue pas en cela une exception.

Ce constat apparaît néanmoins devoir être tempéré compte tenu du fait que les sociétés concernées appartiennent au secteur bancaire et qu'à cet égard les données tant financières que personnelles qu'elles traitent nécessitent des mesures de sécurité renforcées.

Les sociétés du groupe Rothschild soulignent que le dispositif présenté est proportionné à la finalité poursuivie compte tenu notamment des recommandations adoptées par la CNIL dans sa délibération n° 81-094 du 21 juillet 1981 relative aux mesures générales de sécurité des systèmes informatiques dans le cadre de laquelle elle indique qu'il appartient *« aux détenteurs ou utilisateurs de fichiers nominatifs de prendre, sous leur responsabilité, préalablement à toute mise en oeuvre d'une application informatique, compte tenu de la finalité du traitement, du volume des informations traitées et de leur degré de sensibilité au regard des risques d'atteinte à la personne humaine, les mesures générales de sécurité nécessaires […] concernant notamment : […] la capacité de résistance aux atteintes accidentelles ou volontaires extérieures ou intérieures en étudiant particulièrement l'implantation géographique, les conditions d'environnement, les aménagements des locaux et de leurs annexes ».*

Sur ce point, on relèvera également que l'article 34 de la loi du 6 janvier 1978 modifiée en août 2004 impose au responsable du traitement de prendre *« toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »*

De même, les sociétés du groupe Rothschild attirent également l'attention de la Commission sur le fait que l'autorité des marchés financiers recommande *« une prévention maximale quant au risque du délit d'initié, notamment par le biais d'une séparation des serveurs et des métiers de la banque, ce qui nécessite une protection maximale des centres névralgiques de la banque que sont les salles informatiques et la salle téléphonique. »*

Votre rapporteur relève pour sa part qu'aucun des arguments précités ne s'oppose à ce que les sociétés du groupe Rothschild utilisent un dispositif reposant sur la reconnaissance de l'empreinte digitale avec enregistrement dans un support individuel qui apporterait un niveau de sécurité équivalent à celui recherché sans pour autant constituer un risque au regard de la protection des données.

A cet égard, votre rapporteur souligne que, pour la même finalité et en référence à des arguments strictement identiques, la banque Finama a présenté une demande d'autorisation relative à un dispositif reposant sur la reconnaissance de l'empreinte digitale avec stockage sur un support individuel autorisé par la Commission le 2 février 2006 (16).

En outre, votre rapporteur attire l'attention de la Commission sur le fait qu'autoriser les sociétés du groupe Rothschild à utiliser un tel dispositif reviendrait à les mettre au même niveau que la Banque de France, seul « établissement bancaire » jusqu'à présent autorisé à recourir à une base de données d'empreintes digitales pour contrôler l'accès à des zones sensibles (postes de surveillance, locaux de traitement et de conservation des valeurs, plates-formes informatiques réservées aux applications les plus sensibles) (17).

c) Proposition de votre rapporteur

Il résulte de ce qui précède que l'objectif de contrôler l'accès aux salles informatiques, s'il est légitime, n'est associé à aucune circonstance particulière et ne justifie pas dès lors la conservation dans une base de données des empreintes digitales des employés habilités à accéder aux locaux. En conséquence, votre rapporteur propose à la Commission de considérer que le traitement pris dans son ensemble n'apparaît ni adapté ni proportionné à l'objectif poursuivi et ainsi de ne pas autoriser la mise en œuvre des dispositifs présentés.

2. La Mesta Chimie Fine SA

Comme cela a été précédemment indiqué, la Commission doit se prononcer sur une demande d'autorisation modificative (18) dont l'objet est de passer

(16) Délibération n° 2006-022.

(17) Avis favorable n° 97-044 du 10 juin 1997 et délibération n° 2005-023 du 17 février 2005 pour son extension à d'autres sites et l'utilisation de la reconnaissance de l'iris.

(18) Courrier daté du 26 avril 2006.

d'un mode de stockage sur support individuel à un enregistrement des empreintes digitales dans des boîtiers.

La société La Mesta Chimie Fine SA explique sa demande par le fait que le dispositif actuel s'avère inadapté aux contraintes liées à son activité de fabrication de principes actifs pour l'industrie pharmaceutique et au fait que le site dont elle souhaite contrôler les accès relève de la réglementation sur les installations classées pour la protection de l'environnement (ICPE) soumis à une autorisation d'exploiter préfectorale.

S'agissant d'un site classé de type « SEVESO seuil bas » dans lequel sont stockés simultanément des produits dangereux, la société La Mesta Chimie Fine SAS a obligation de mettre en œuvre un Plan d'Opération Interne (POI) dans lequel sont définis les mesures d'organisation et les moyens à mobiliser pour protéger le personnel, la population et l'environnement en cas d'accident. A ce titre, la société La Mesta Chimie Fine SAS doit être en mesure de fournir, en cas d'exercice d'évacuation ou d'accident, la liste exacte des personnes présentes sur le site. Ainsi, outre le renforcement des conditions d'accès au site, le dispositif biométrique doit lui permettre de garantir la fiabilité de cette liste.

C'est ce second objectif que le dispositif impliquant l'utilisation d'une carte ne permet pas de garantir. En effet, en cas de perte, de vol ou d'endommagement des cartes les employés feront alors appel à un collègue déjà présent sur le site afin de pouvoir y entrer et échappent alors au décompte en cas d'exercice ou d'accident.

Compte tenu d'une part, du fort impératif de sécurité lié à la nécessité de contrôler l'accès à un site classé de type « SEVESO » dans lequel sont stockés simultanément des produits dangereux et, d'autre part, de l'obligation de fournir, en cas d'exercice d'évacuation ou d'accident, la liste exacte des personnes présentes sur le site, votre rapporteur propose à la Commission de considérer que le traitement et notamment, le recours à la constitution d'une base de données biométrique, est adapté et proportionné à la finalité assignée au dispositif et peut en conséquence être autorisé.

Hubert Bouchet

ANNEXE : **Liste des dispositifs reposant sur la reconnaissance des empreintes digitales avec enregistrement dans une base de données dont la mise en œuvre a été acceptée par la Commission**

Responsable du traitement	Finalité	Contexte	Décision de la CNIL	Caractéristiques techniques	Modalités de stockage	Commentaires
Banque de France	Contrôle d'accès	Zones hautement sécurisées	Avis favorable n° 97-044 du 10 juin 1997	Sas à unicité de passage équipé d'un appareil " fingerscan " (IDENTIX)	Base de données centralisée	
Cité académique de Lille	Contrôle d'accès de certains personnels de l'Education nationale à certains locaux	Confidentialité des sujets d'examens et concours notamment	Avis favorable n° 00-056 du 16 novembre 2000 DA 709756	Technologie SAGE - BIOTIME (boîtiers " morphotouch "de la SAGEM), installée par la société PROFABEL SEMLEX	Base de données centralisée	
COGEMA La Hague	Contrôle d'accès	Zones sensibles (bâtiments de stockage du plutonium)	Examen en séance plénière des 26/10 et 16/11/2000 Récépissé du 17 novembre 2000	Sas avec lecteur biométrique et PC pour saisie du n° de badge personnel Société GET	Base de données centralisée	
SAGEM	Contrôle d'accès	Sécurisation de l'accès aux zones de fabrication de cartes à puce	Récépissé du 25 avril 2001	SAGEM	Base de données centralisée	Utilisation à titre expérimental (six mois) et sur la base du volontariat Bilan demandé à l'issue de l'expérimentation
Aéroports de Paris	Contrôle des accès des personnels d'ADP et des services publics ou des entreprises intervenant en zones réservées sûreté	Sécurisation des "zones réservées sûreté" (ZRS) des aéroports de Roissy et d'Orly	Avis favorable 02-034 du 23 avril 2002 (DA 799468)	SAGEM Morphoaccess ou Morphotouch pour l'empreinte digitale	Pendant l'expérimentation : stockage sur une base de données centralisée. A terme : stockage sur carte à puce	Utilisation sur la base du volontariat s'agissant de l'accès au bâtiment et obligatoire s'agissant de l'accès aux trois étages sensibles
SAGEM SA	Contrôle des accès	Activités classées "secret défense" et "secret OTAN"	Récépissé du 13 mai 2002 (DO 769 366)	Morphoaccess MA 300 et Morphoaccess MA 200 / Installateur CEGELEC	Base de données centralisée	
CCI de Nice-Côte d'Azur	Contrôle d'accès	Sécurisation des bases de données et des équipements	Demande de complément décidée en séance plénière du 8 avril 2004. Suite à réception du complément d'information, avis tacite favorable (07/2004)	Lecteurs ZX20 (Société ZALIX), avec logiciels Bioacess / Biologon	Base de données centralisée chiffrée et stockée sur un poste dédié	

Groupe Imprimerie nationale	Contrôler l'accès du site où sont produits les passeports, les cartes grises et les cartes d'identité	Sécuriser l'émission des documents officiels	Autorisation n° 2005-113 du 7 juin 2005	Sagem	Base de données centralisée	
INHES Institut National des Hautes Etudes de Sécurité	Contrôle d'accès	Cloisonner les zones accessibles au public de celles dans lesquelles sont situées des informations sensibles / confidentielles défense	Autorisation n° 2005-149 du 14 juin 2005	Sagem	Base de données centralisée (serveur)	
Sagem Défense Sécurité	Contrôle d'accès	Sécurisation des zones sensibles / secret défense	Autorisation n° 2006-070 du 16 mars 2006	Sagem	Base de données centralisée (serveur)	Site de Montluçon
ATM	Contrôle d'accès	Sécurisation des zones dans lesquelles sont situés des documents secret / confidentiel défense	Autorisation n° 2006-068 du 16 mars 2006	Sagem	Base de données centralisée (serveur)	Etablissement prestataire de service pour la Cogema et agréé par le CEA

NB : les trois dossiers SAGEM correspondent à des sites différents.

Annexe

LIBERTES ET DROITS FONDAMENTAUX – Dispositifs de contrôle des salariés – Système biométriques – Appréciation des atteintes (deux espèces).

Première espèce : **Commission nationale de l'informatique et des libertés**

Délibération 2006-153 du 30 mai 2006

Délibération portant refus d'autorisation de la mise en oeuvre par la société Rothschild et Compagnie Banque d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux.

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment son article 25-8° ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu la demande d'autorisation, présentée par la société Rothschild & Compagnie Banque d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux ;

Formule les observations suivantes :

Le 23 septembre 2005, la société Rothschild & Compagnie Banque a adressé à la Commission nationale de l'informatique et des libertés une déclaration relative à la mise en œuvre d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et dont la finalité est de sécuriser l'accès aux salles dans lesquelles sont situés les équipements informatiques et téléphoniques.

La Commission considère qu'il y a lieu de faire application des dispositions de l'article 25-8° de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

Il convient d'examiner ledit traitement au regard des principes relatifs à la protection des données à caractère personnel, et notamment, de l'article 6-3° de la loi du 6 janvier 1978 modifiée qui dispose que les traitements ne peuvent porter que sur des données à caractère personnel adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs.

Les empreintes digitales sont des données biométriques qui laissent des traces pouvant ensuite être exploitées à des fins d'identification de personnes. Dès lors la constitution et l'utilisation de bases de données nominatives associées à des empreintes digitales, même limitées à la comparaison des empreintes aux seules fins de contrôle d'accès à des locaux ou à des services, comportent un risque d'atteinte aux libertés individuelles dans la mesure où elles sont susceptibles d'être utilisées à des fins étrangères à la finalité initialement poursuivie.

La Commission estime en conséquence que la constitution de bases de données d'empreintes digitales, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles de ces bases de données, ne peut être admise que dans certaines circonstances particulières où l'exigence de sécurité et d'identification des personnes est impérieuse.

Or, en l'espèce, l'objectif invoqué par la société Rothschild & Compagnie Banque de contrôler l'accès aux salles dans lesquelles sont situés les équipements informatiques et téléphoniques, s'il est légitime, ne justifie pas la conservation dans une base de données des empreintes digitales des employés habilités à accéder aux locaux. Ce contrôle d'accès pourrait tout aussi bien être assuré au moyen d'un dispositif de reconnaissance des empreintes digitales avec enregistrement sur un support individuel, qui ne présente pas les mêmes risques en termes de protection des données. En conséquence, le traitement pris dans son ensemble n'apparaît ni adapté ni proportionné à l'objectif poursuivi.

Dès lors, la Commission n'autorise pas la société Rothschild & Compagnie Banque, sise 17 avenue Matignon - 75008 Paris, à mettre en oeuvre un traitement de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance des empreintes digitales et dont la finalité est de sécuriser l'accès aux salles dans lesquelles sont situés les équipements informatiques et téléphoniques.

(M. Türk, prés. - M. Bouchet, rapp. - Mme Compagnie, comm. gouv.)

Deuxième espèce : **Commission nationale de l'informatique et des libertés**

Délibération 2006-158 du 30 mai 2006

Délibération portant autorisation de la mise en œuvre par la société La Mesta Chimie Fine SAS d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux.

Le 26 avril 2006, la société La Mesta Chimie Fine SAS, a adressé à la Commission nationale de l'informatique et des libertés une demande d'autorisation portant modification du dispositif de reconnaissance des empreintes digitales ayant pour finalité le contrôle de l'accès aux locaux dont la mise en oeuvre avait été autorisée par la délibération numéro 2006-071 du 16 mars 2006.

Cette demande a principalement pour objet la modification des modalités de stockage des empreintes digitales des employés concernés. Ainsi, la société La Mesta Chimie Fine SA souhaite désormais enregistrer les empreintes digitales des employés dans une base de données et non plus au sein d'un support individuel comme cela était le cas précédemment.

La Commission considère que la modification des fonctions générales du traitement, en l'espèce des modalités de stockage des empreintes digitales, porte sur l'un des éléments visés au 2° du 1 de l'article 30 de la loi du 6 janvier 1978 modifiée et constitue une modification de caractère substantiel. En conséquence, il y a lieu pour la Commission de faire application de l'article 25-8° de la loi du 6 janvier 1978 modifiée en août 2004 qui soumet à autorisation les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

La société La Mesta Chimie Fine SA, spécialisée dans la fabrication de principes actifs pour l'industrie pharmaceutique, précise que le dispositif reposant sur l'utilisation d'une carte à puce s'est avéré inadapté aux contraintes liées au fait que le site dont elle souhaite contrôler les accès relève de la réglementation sur les installations classées pour la protection de l'environnement (ICPE) soumis à une autorisation d'exploiter préfectorale.

S'agissant d'un site classé de type "SEVESO seuil bas" dans lequel sont stockés simultanément des produits dangereux, la société La Mesta Chimie Fine SAS a obligation de mettre en oeuvre un Plan d'Opération Interne (POI) dans lequel sont définis les mesures d'organisation et les moyens à mobiliser pour protéger le personnel, la population et l'environnement en cas d'accident. A ce titre, la société La Mesta Chimie Fine SAS doit être en mesure de fournir, en cas d'exercice d'évacuation ou d'accident, la liste exacte des personnes présentes sur le site.

Or, le recours à un support individuel de stockage des empreintes digitales ne permet pas de savoir quelles sont les personnes présentes sur les lieux en cas d'oubli, de perte, de vol ou d'endommagement des cartes. Dès lors, afin d'assurer le suivi exhaustif des personnes accédant au site et de garantir la fiabilité de l'historique de leurs passages, la modification du dispositif apparaît nécessaire.

Ainsi, le dispositif modifié reposera sur plusieurs boîtiers répartis aux différents points d'accès au site et au local de maintenance. Les gabarits des empreintes digitales des personnes habilitées à accéder au site et au local de maintenance seront enregistrés dans ces boîtiers. Ces derniers seront reliés à un serveur au niveau duquel seront enregistrés l'identité des employés (nom, prénom). Lors du contrôle d'accès, l'employé apposera son doigt sur le lecteur biométrique du boîtier, une comparaison s'effectuera alors entre cette empreinte digitale et le gabarit enregistré dans la base de données du lecteur.

Les données relatives à l'historique des passages seront conservées pendant un mois. La durée de conservation relative à l'identité de l'employé et au gabarit de l'empreinte digitale, sera égale au temps pendant lequel la personne concernée travaille pour la société Mesta Chimie Fine.

Une information et une consultation du comité d'entreprise ont été effectuées conformément aux dispositions de l'article L. 432-2 du Code du travail. L'information individuelle des employés est effectuée au moment de l'enrôlement. Les employés peuvent accéder en ligne à leur dossier comportant l'historique de leurs passages après saisie d'un mot de passe et d'un nom d'utilisateur.

Enfin, les mesures prises en vue de garantir la sécurité des données, apparaissent conformes à l'état de l'art et aux exigences de la Commission. S'agissant du contrôle d'accès logique au système, les éléments d'informations figurant dans les dossiers apparaissent satisfaisants notamment, concernant l'administration des mots de passe et la politique de gestion des accès dans la mesure où, seuls le responsable hygiène et sécurité et le chef de service administratif disposent de l'habilitation pour accéder aux données. Enfin, il convient de préciser d'une part, que l'accès à l'application et aux fichiers contenant les données à caractère personnel fera l'objet d'une journalisation et, d'autre part, que le dispositif repose sur un réseau privé permettant de prévenir tout risque d'intrusion extérieure.

Compte tenu d'une part, du fort impératif de sécurité lié à la nécessité de contrôler l'accès à un site classé de type "SEVESO" dans lequel sont stockés simultanément des produits dangereux et, d'autre part, de l'obligation de fournir la liste exacte des personnes présentes sur le site, les traitements et notamment, le recours à la constitution de bases de données biométriques, sont adaptés et proportionnés à la finalité assignée au dispositif.

Les droits d'accès et de rectification s'exerceront auprès du directeur administratif et financier de la société La Mesta Chimie Fine SAS, sise Pont Charles Albert - 06830 Gilette.

Les catégories de données à caractère personnel enregistrées seront l'identité des employés (nom, prénom), le gabarit de leur empreinte digitale et l'historique des passages.

Les destinataires des informations seront, dans la limite de leurs attributions respectives et pour la poursuite de la finalité précitée, le responsable hygiène et sécurité et le chef de service administratif.

Autorise, dans ces conditions, la société La Mesta Chimie Fine SAS à mettre en œuvre le traitement de données à caractère personnel présenté.

(M. Türk, prés. - M. Bouchet, rapp. - Mme Compagnie, comm. gouv.)